

Schriftenreihe
Forschungsforum Öffentliche Sicherheit

# State of the Art der Forschung zur Verwundbarkeit Kritischer Infrastrukturen am Beispiel Strom/Stromausfall

J. Birkmann, C. Bach, S. Guhl,
M. Witting, T. Welle, M. Schmude









GEFÖRDERT VOM






# State of the Art der Forschung zur Verwundbarkeit Kritischer Infrastrukturen am Beispiel Strom/Stromausfall

J. Birkmann, C. Bach, S. Guhl,
M. Witting, T. Welle, M. Schmude





Forschungsforum Öffentliche Sicherheit

Schriftenreihe Sicherheit Nr. 2
Oktober 2010
ISBN: 978-3-929619-63-8

---

Anschrift:
Freie Universität Berlin
Fabeckstr. 15
14195 Berlin

Tel: +49 (0)30 838 57367
Fax: +49 (0)30 838 57399
www.schriftenreihe-sicherheit.de
kontakt@schriftenreihe-sicherheit.de

---

Über die Autoren

---

Priv.-Doz. Dr. Jörn Birkmann
Jörn Birkmann ist Leiter der Sektion „Vulnerability Assessment, Risk Management & Adaptive Planning" bei UNU-EHS. Außerdem ist er Leitautor im Rahmen des fünften IPCC Sachstandsberichts.

Claudia Bach
Claudia Bach studierte an der Leibniz Universität Hannover European Studies und ist als Research Associate im KIBEX-Projekt bei UNU-EHS tätig.

Silvie Guhl
Silvie Guhl studierte an der Rheinischen Friedrich-Wilhelms-Universität Bonn Geographie und ist als Research Associate bei UNU-EHS tätig.

Maximilian Witting
Maximilian Witting studiert seit 2005 an der Rheinischen Friedrich-Wilhelms-Universität Bonn Geographie und ist bei UNU-EHS als studentische Hilfskraft eingestellt.

Dr. Torsten Welle
Torsten Welle studierte an der Rheinischen Friedrich-Wilhelms-Universität Bonn Geographie und promovierte im Fach Geographie an der Universität Bonn. Er ist als Associate Academic Officer bei UNU-EHS tätig.

Miron Schmude
Miron Schmude studiert seit 2005 an der Rheinischen Friedrich-Wilhelms-Universität Bonn Geographie und ist bei UNU-EHS als Praktikant eingestellt.

Kontakt zum Autor:

---

United Nations University
Institute for Environment and Human Security(UNU-EHS)
PD Dr. Jörn Birkmann
Claudia Bach
Langer Eugen – UN Campus
Hermann- Ehlers-Strasse 10
53113 Bonn

Tel: +49-228-815-0208
Tel: +49-228-815-0230
Fax: +49-228-815-0299
E-Mail: birkmann@ehs.unu.edu
E-Mail: bach@ehs.unu.edu





## Inhaltsverzeichnis

1 Einleitung ....... 13

2 Die Entwicklung der Stromversorgung in Deutschland als Beispiel einer Kritischen Infrastruktur ....... 19

3 Das Konzept der Verwundbarkeit ....... 25

3.1 Definitionen ....... 25

3.2 Konzepte der Verwundbarkeit ....... 26

3.2.1 Das BBC-Framework ....... 28

3.2.2 Verwundbarkeitsmodell für gekoppelte Mensch-Umwelt-Systeme nach Turner ....... 30

3.3 Konzepte zur Verwundbarkeit Kritischer Infrastrukturen ....... 32

3.3.1 Verwundbarkeitsbemessung nach Holmgren ....... 33

3.3.2 Verwundbarkeitsanalyse nach Krings ....... 34

3.3.3 Verwundbarkeitsabschätzung nach Baker ....... 36

4 Verwundbarkeit der Elektrizitätsversorgung ....... 39

4.1 Exposition ....... 39

4.1.1 Naturgefahren ....... 39

4.1.2 Kriminelle Handlungen ....... 47

4.1.3 Übersicht einiger Stromausfälle ....... 55

4.1.4 Zwischenfazit Exposition ....... 61

4.2 Anfälligkeit ....... 64

4.3 Bewältigungskapazität ....... 73

5 Verwundbarkeit des Systems „KRITIS-Mensch“ ....... 81

5.1 Abhängigkeit anderer KRITIS von der Elektrizitätsversorgung ....... 81

5.2 Abhängigkeit der Bevölkerung von Kritischer Elektrizitätsinfrastruktur ....... 83

5.3 Erfassung der Komplexität ....... 87



5.4 Analyse der Ausfälle der Vergangenheit ..... 91

5.5 Zwischenfazit des Systems „KRITIS-Mensch“ ..... 94

6 Staatliche und privatwirtschaftliche Handlungsmöglichkeiten zur Förderung der Resilienz Kritischer Infrastrukturen ..... 95

6.1 Exposition ..... 95

6.1.1 Exposition gegenüber Naturgefahren ..... 95

6.1.2 Exposition gegenüber kriminellen Handlungen ..... 96

6.2 Anfälligkeit ..... 100

6.2.1 Institutionelle Faktoren ..... 100

6.2.2 Systemische Faktoren ..... 102

6.2.3 Technologische Faktoren ..... 102

6.2.4 Menschliche Faktoren ..... 103

6.3 Bewältigungskapazität ..... 104

6.3.1 Prävention ..... 104

6.3.2 Reaktion ..... 104

6.3.3 Möglichkeiten durch erneuerbare Energien ..... 105

6.4 Risk Governance ..... 112

7 Fazit ..... 119

Anhang 1: Dimensionen der Wirkzusammenhänge nach Rinaldi et al. (2001) ..... 123

8 Literaturverzeichnis ..... 127



## Abbildungsverzeichnis


Abbildung 1: Anzahl der großen Naturkatastrophen 1950 – 2008 ................................15

Abbildung 2: Regelzonen Deutscher Übertragungsnetzbetreiber, 1997 und heute ........19

Abbildung 3: Brutto Stromerzeugung nach Energieträgern in Deutschland 2009 .........20

Abbildung 4: Stromnetz in Europa im 20. Jahrhundert ................................................22

Abbildung 5: BBC Rahmenkonzept.............................................................................29

Abbildung 6: Gekoppeltes Mensch-Umwelt-System nach Turner ................................31

Abbildung 7: Schematische Darstellung zur Erfassung der Verwundbarkeit von KRITIS-Komponenten .............................................................................35

Abbildung 8: Verwundbarkeitsabschätzung nach Baker ..............................................37

Abbildung 9: Naturräumliche Gliederung Deutschlands ..............................................44

Abbildung 10: Strommasten knicken um wie Streichhölzer.........................................46

Abbildung 11: Risikokarte Deutschland: Kernkraftwerke............................................49

Abbildung 12: INES – International Nuclear Event Scale............................................50

Abbildung 13: Unterschiedliche Konfliktformen im Internet........................................52

Abbildung 14: Schematische Teilung des UCTE Netzes in drei Gebiete......................60

Abbildung 15: Übertragbarkeit der Ursachen für Stromausfälle in das Konzept der Vulnerabilität...............................................................................65

Abbildung 16: Grenzüberschreitende Energieflüsse in Europa in GWh ........................66

Abbildung 17: Organisationsstruktur des Elektrizitätssystems vor der Liberalisierung.67

Abbildung 18: Organisationsstruktur eines liberalisierten Elektrizitätssystems (dezentralisiertes Modell)...........................................................................68

Abbildung 19: Indikatoren der Bewältigungskapazität.................................................73

Abbildung 20: Redundanz..........................................................................................75

Abbildung 21: Die dezentrale Elektrizitätsversorgung – Elemente eines vernetzten Systems ......................................................................................79



Abbildung 22: Interaktionsschema zu Umweltbedingungen, Bevölkerung und KRITIS unter dem Einfluss des Klimawandels ............................................................ 81

Abbildung 23: Auswirkungen eines Stromausfalls auf andere KRITIS ......................... 82

Abbildung 24: Mögliche Auswirkungen eines Stromausfalls ....................................... 83

Abbildung 25: Bedeutung der Stromversorgung .......................................................... 84

Abbildung 26: Interdependenzen von Basis-, sozioökonomischen und soziokulturellen Infrastrukturen.......................................................................................................... 87

Abbildung 27: Dimensionen der Interdependenzen Kritischer Infrastrukturen.............. 88

Abbildung 28: Störungen mit Versorgungsunterbrechungen im Mittelspannungsnetz .. 92

Abbildung 29: Ursächliche Komponenten für Stromausfälle ........................................ 93

Abbildung 30: Bruttostromerzeugung nach Energieträgern in Deutschland ................ 106

Abbildung 31: Struktur der Stromerzeugung aus erneuerbaren Energien in Deutschland im Jahr 2009 .......................................................................................................... 108

Abbildung 32: Smart Grids ......................................................................................... 110

Abbildung 33: Von der heutigen, zentralisierten Stromversorgung zu einem vernetzten Stromnetz mit zentralen und dezentralen Produktionsanlagen .................................... 111

Abbildung 34: Sieben Schritte einer Risiko-Kette: Das Beispiel Atomenergie ........... 113

Abbildung 35: IRGC Risk Governance Framework .................................................... 114

Abbildung 36: Risk Management und Risikosteuerung .............................................. 117



## Tabellenverzeichnis

Tabelle 1: Elemente der öffentlichen Stromversorgung ................................................ 23

Tabelle 2: Komponenten der Verwundbarkeit Kritischer Infrastrukturen und ausgewählte Beispiele ........................................................................................................ 38

Tabelle 3: Übersicht über mögliche Naturgefahren und ihre räumliche sowie zeitliche Komponente ............................................................................................................. 40

Tabelle 4: Überblick ausgewählter Stromausfälle ......................................................... 56

Tabelle 5: Gesamtübersicht der mittleren Nichtverfügbarkeit je Netzkunde und Jahr (SAIDI) ..................................................................................................................... 91

Tabelle 6: Risikocharakteristika und ihre Auswirkungen auf das Risk Management .. 115



## Abkürzungsverzeichnis

| | |
|---|---|
| A | Ampere |
| AC | Wechselstrom |
| AEUV | Vertrag über die Arbeitsweise der Europäischen Union |
| AG KRITIS | Arbeitsgemeinschaft Kritische Infrastrukturen |
| ALARA | as low as reasonably achievable |
| ALARP | as low as reasonable practicable |
| Art. | Artikel |
| BACT | best available control technology |
| BBC | Bogardi, Birkmann und Cardona |
| BBK | Bundesamt für Bevölkerungsschutz und Katastrophenhilfe |
| BDEW | Bundesverband der Energie- und Wasserwirtschaft e.V. |
| BfG | Bundesanstalt für Gewässerkunde |
| BfS | Bundesamt für Strahlensicherheit |
| BKA | Bundeskriminalamt |
| BMI | Bundesministerium des Innern |
| BMU | Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit |
| BMWi | Bundesministerium für Wirtschaft und Technologie |
| BSI | Bundesamt für Sicherheit in der Informationstechnik |
| Bsp. | Beispiel |
| C | Celsius |
| CIA | Central Intelligence Agency |
| CIWIN | Critical Infrastructure Warning Information Network |
| CONSENTEC | Consulting für Energiewirtschaft und –technik GmbH |
| CYTEX | Cyber Terror Exercise |
| DDoS | Distributed Denial of Service |
| Destatis | Statisches Bundesamt Deutschland |
| DIN | Deutsche Industrie-Norm |
| DKKV | Deutsches Komitee Katastrophenvorsorge e.V. |
| DoS | Denial of Service |
| EC | European Commission |
| EEG | Erneuerbaren-Energien-Gesetz |
| EG | Europäische Gemeinschaft |
| EGV | Vertrag zur Gründung der Europäischen Gemeinschaft |
| EN | Europäische Norm |
| EnBW | Energie Baden-Württemberg AG |
| ENTSO-E | European Network of Transmission System Operators for Electricity |
| EnWG | Energiewirtschaftsgesetz |
| EO | Executive Order |
| EPSKI | Europäisches Programm für den Schutz Kritischer Infrastrukturen |



| | |
|---|---|
| et al. | und andere |
| EU | Europäische Union |
| EWI | Energiewissenschaftliches Institutan der Universität zu Köln |
| f | folgende |
| FAZ | Frankfurter Allgemeine Zeitung |
| ff | fortfolgende |
| FOI | Swedish Defence Research Agency |
| gem. | gemäß |
| GIG-BE | Global Information Grid Bandwidth Expansion |
| GmbH | Gesellschaft mit beschränkter Haftung |
| GPS | Global Positioning System |
| GRS | Gesellschaft für Anlagen- und Reaktorsicherheit mbH |
| GWh | Gigawattstunde |
| HTTP | Hypertext Transfer Protocol |
| IAEA | International Atomic Energy Agency |
| IAEW | Institut für Elektrische Anlagenund Energiewirtschaftder RWTH Aachen |
| IHK | Industrie- und Handelskammer |
| IKT | Informations- und Kommunikationstechnik |
| INES | International Nuclear Event Scale |
| IPCC | Intergovernmental Panel on Climate Change |
| IRGC | International Risk Governance Council |
| IT | Informationstechnik |
| IuK | Information und Kommunikation |
| KKW | Kernkraftwerk |
| km | Kilometer |
| KOM | Kommision |
| KRITIS | Kritische Infrastrukturen |
| kV | Kilovolt |
| kWh | Kilowattstunde |
| LÜKEX | Länder Übergreifende Krisenmanagement-Übung/Exercise |
| MELANI | Melde- und Analysestelle Informationssicherung |
| min/a | Minuten pro Jahr |
| Mio. | Million |
| Mrd. | Milliarde |
| MS | Mittelspannung |
| MW | Megawatt |
| MWh | Megawattstunde |
| NATO | North Atlantic Treaty Organization |
| NS | Niederspannung |
| NPS | Naval Postgraduate School |



| | |
|---|---|
| NSA | National Security Agency |
| ÖPNV | Öffentlicher Personennahverkehr |
| PC | Personal Computer |
| PCCIP | President’s Commission on Critical Infrastructure Protection |
| PPP | Public Private Partnership |
| REVU | Regionalversorgungsunternehmen |
| RL | Richtlinie |
| RWE | Rheinisch-Westfälisches Elektrizitätswerk AG |
| S. | Seite |
| s.o. | siehe oben |
| SAIDI | System Average Interruption Duration Index |
| SCADA | Supervisory Control and Data Aquisition |
| TWh | Terawattstunde |
| UCTE | Union for the Co-ordination of Transmission of Electricity |
| UN/ISDR | United Nations International Strategy for Disaster Reduction |
| UNDP | United Nations Development Programme |
| USV | unterbrechungsfreie Stromversorgung |
| usw. | und so weiter |
| VDE | Verband der Elektrotechnik, Elektronik und Informationstechnik |
| VDN | Verband der Netzbetreiber |
| vgl. | vergleiche |
| vs. | versus |
| WLAN | Wireless Local Area Network |
| z.B. | zum Beispiel |



# 1 Einleitung

Kritische Infrastrukturen (KRITIS) sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten können (BMI, 2005, S. 6). Diese Definition verdeutlicht die besondere Funktion, die Kritische Infrastrukturen für das Funktionieren der Gesellschaft haben. Der Elektrizitätsversorgung, deren Verwundbarkeit im Rahmen dieser Studie analysiert wird, kommt dabei eine besondere Bedeutung zu, da sie als Basisinfrastruktur vielfach die Grundlage für die Funktionsfähigkeit anderer Infrastrukturdienstleistungen, wie beispielsweise Informations- und Telekommunikationstechnologien, Trinkwasserver- und Abwasser-entsorgung oder das Notfall- und Rettungswesen bildet (BMI, 2005, S. 5).

Verdeutlicht wurde dies durch den Stromausfall im Münsterland im November 2005. Durch das Sturmtief *Torsten* wurden Hochspannungsmasten und -leitungen schwer beschädigt. In diesem Zusammenhang mussten weitere Trassenabschnitte aus Sicherheitsgründen abgeschaltet werden. Dies führte dazu, dass für etwa 250.000 Menschen bei Temperaturen um den Gefrierpunkt der Strom ausfiel. Auch vier Tage später waren immer noch rund 20.000 Personen von der Stromversorgung abge-schnitten. Während dieser Unterbrechung stellte sowohl die Koordination der Versorgung der Bevölkerung, als auch der Betrieb von Notstromgeräten in Krankenhäusern, Altenheimen oder Melkständen der Bauernhöfe eine erhebliche Herausforderung für den Bevölkerungsschutz dar. Viele Haushalte waren nur schlecht mit Lebensmittelvorräten versorgt (Birkmann & Krings, 2008; Menski & Gardemann, 2008).

Dieses Beispiel zeigt, welche Konsequenzen ein Stromausfall für die Gesellschaft haben kann. Es wird deutlich, dass die zunehmende Abhängigkeit der Bevölkerung und Wirtschaft von KRITIS und hier insbesondere von der Elektrizitätsversorgung auch eine erhebliche Schwachstelle bildet. Die zunehmende Nutzung von Elektrizität für zahlreiche Prozesse des Alltags- und Wirtschaftslebens in industrialisierten und hochentwickelten Ländern kann dabei als Paradox begriffen werden, da hierdurch die Verwundbarkeit der Gesellschaft im Störfall erhöht wird. Es ist daher von besonderem Interesse, die Verwundbarkeit[1] dieser KRITIS näher zu beleuchten.

Im Kontext der Risikoforschung gegenüber Naturgefahren wird Vulnerabilität als die von physischen, sozialen, ökonomischen und ökologischen Faktoren und Prozessen bestimmte Gegebenheit, die die Anfälligkeit einer Gesellschaft gegenüber Gefahren

[1] Die Begriffe Verwundbarkeit und Vulnerabilität werden im Folgenden synonym verwendet.



(Hazards) erhöhen (UN/ISDR 2004, eigene Übersetzung), definiert. Um den Grad der Verwundbarkeit einer Gesellschaft, bzw. eines Systems abschätzen zu können, müssen verschiedene Komponenten berücksichtigt und klar definiert werden (Kapitel 3). Vulnerabilität geht in der neuesten wissenschaftlichen Diskussion deutlich über die Frage der Verletzlichkeit hinaus und betrachtet auch Aspekte der Exposition und Bewältigung (siehe u.a. Turner et al., 2003; Birkmann, 2006; Adger, 2006). Ein wichtiger Ansatzpunkt, um Vulnerabilität greifbar zu machen, wurde von Birkmann (2006) entwickelt, der sie als Funktion aus *Exposition* gegenüber einer *Gefahr, Anfälligkeit* und *Bewältigungskapazität* definiert (Birkmann, 2006):

| f (Vulnerabilität) = Exposition (Gefahr), Anfälligkeit, Bewältigungskapazität |
|---|

Dieses Konzept wurde allerdings primär im Zusammenhang mit der Naturrisikoforschung entwickelt, sodass es im Weiteren für den Gegenstand der KRITIS weiter ausformuliert und angepasst werden muss (Kapitel 3). Die *Exposition* der KRITIS-Komponenten ist je nach Gefahr unterschiedlich, wobei diese sich in Naturgefahren und in von Menschen verursachten Gefahren untergliedern lassen. Die von Menschen verursachten Gefahren schließen dabei Terrorismus und Cyberattacken ein. In diesem Feld ist insbesondere seit dem 11. September 2001 die Bedrohung durch den internationalen Terrorismus in den Fokus möglicher Ereignisse gerückt, die zum Ausfall oder zur Zerstörung von KRITIS führen können (BMI, 2009, S. 7). Jedoch nimmt auch die Anzahl der weltweiten großen Katastrophen im Kontext von Naturgefahren[2] seit 1950 stark zu (Münchener Rück, 2009, S. 39). Dieser Trend wird sich auch im Zuge des Klimawandels tendenziell weiter fortsetzen (IPPC, 2007a, S. 783). In den nördlichen mittleren Breitengeraden ist dabei insbesondere mit heißeren Sommern zu rechnen, die zunehmend auch mit Starkregenfällen und Überschwemmungen einhergehen können, da die wärmere Luft mehr Feuchtigkeit speichern kann. Die Ausprägung der Extremereignisse wird dabei neben einer grundsätzlichen Verschiebung der Niederschläge vom Sommer in den Herbst vermutlich zunehmen (IPPC, 2007a, S. 783).

[2] Als Katastrophen gelten Naturereignisse dann, wenn die Gesellschaft in starkem Maße geschädigt wurde, die Selbsthilfefähigkeit der betroffenen Regionen deutlich überschritten und überregionale oder internationale Hilfe erforderlich ist. Dies ist meist dann der Fall, wenn die Zahl der Todesopfer in die Tausende, die Zahl der Obdachlosen in die Hunderttausende geht und/oder, wenn die Gesamtschäden – gemessen an den wirtschaftlichen Verhältnissen des betroffenen Landes – und/oder die versicherten Schäden außergewöhnliche Größenordnungen erreichen. (Münchener Rück, 2009, S. 38) Die Zunahme der Katastrohpen trifft jedoch noch keine Aussage über die tatsächliche Häufigkeit und Instensität der Naturereignisse, sondern spiegelt die Verwundbarkeit der Gesellschaft wider.



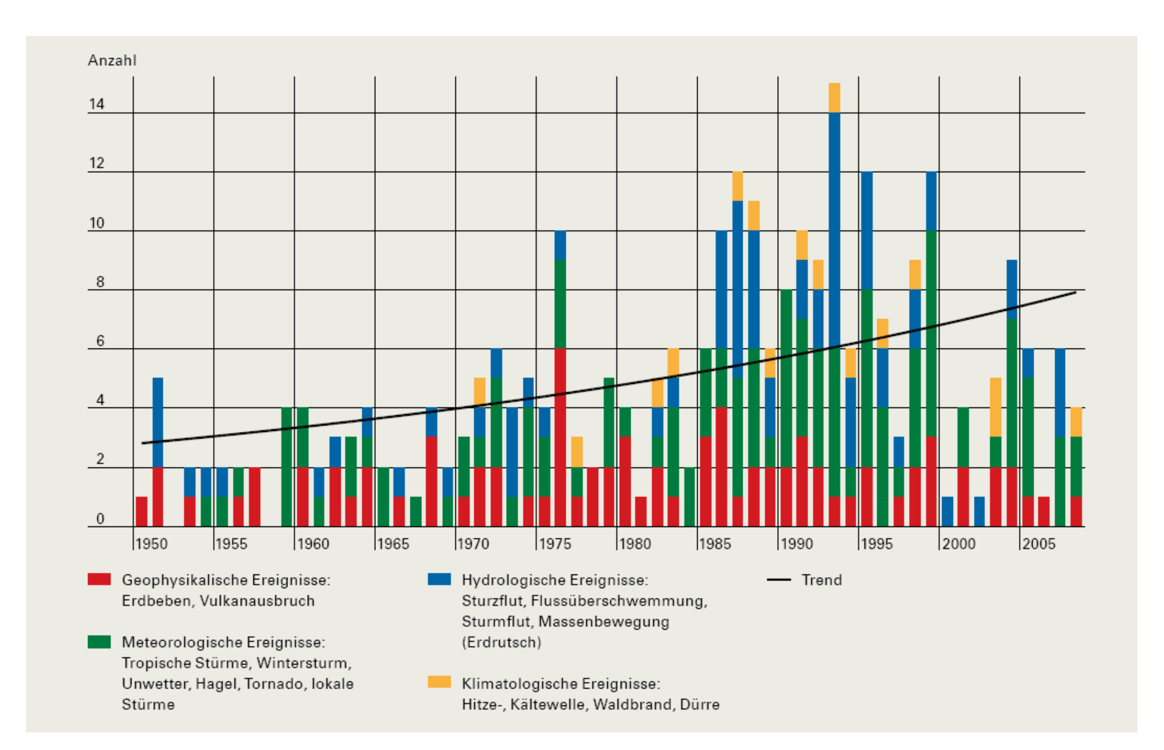



**Abbildung 1: Anzahl der großen[3] Naturkatastrophen 1950 – 2008**

Quelle: (Münchener Rück, 2009, S. 39)

Diese Entwicklungen zeigen, dass die Exposition von KRITIS gegenüber Naturgefahren und sog. Extremwetterereignissen tendenziell wächst. Eine detaillierte Analyse der Exposition von Elektrizitätsinfrastruktur gegenüber verschiedenen Gefahren wird in Kapitel 4.1 vorgenommen.

Die *Anfälligkeit* von KRITIS gegenüber unterschiedlichen Gefahren kann durch verschiedene Faktoren beeinflusst werden (siehe Kapitel 4.2). Hierzu gehört zunächst die Qualität der Komponenten und die Frage, ob diese physisch in der Lage sind unterschiedlichen Gefahren standzuhalten. Neben den Komponenten, die die Stromversorgung umfasst, sind Prozesse wie Stromerzeugung, Umspannung, sowie Transport wichtig, die im Ereignisfall ausfallen können. Diese Prozesse werden u.a. von institutionellen Faktoren beeinflusst, wobei insbesondere die Privatisierung und Liberalisierung des Energiemarktes betrachtet werden. Ferner wird auch die Bedeutung menschlicher (z.B. menschliches Versagen), technischer (z.B. Verwendung bestimmter Software) und systemischer Faktoren im Rahmen eines integrierten Vulnerabilitätsassessments zu berücksichtigen sein. Letztere sind durch die zunehmende Komplexität der Elektrizitätsversorgung und den Anstieg der Abhängigkeit von anderen

[3] Das Diagramm zeigt für jedes Jahr die Anzahl der Großkatastrophen der Kategorie 6, unterteilt nach Ereignistypen. Als „groß" bezeichnet man Naturkatastrophen in Anlehnung an die Definitionen der Vereinten Nationen dann, wenn die Selbsthilfefähigkeit der betroffenen Regionen deutlich überschritten und überregionale oder internationale Hilfe erforderlich ist. Siehe auch Fußnote 2 auf Seite 2.



Infrastrukturdienstleistungen wie z.B. IT gekennzeichnet. Ferner kann das Konsumverhalten der Bevölkerung die Anfälligkeit der Elektrizitätsversorgung beeinflussen, beispielsweise durch eine erhöhte Nachfrage durch Klimaanlagen im Sommer, der die Betreiber bei möglicherweise verringerter Kraftwerksleistung gerecht werden müssen.

Der Grad der *Bewältigungskapazität* der Elektrizitätsversorgung lässt sich durch die im Kapitel 4.3 im Detail erläuterten Faktoren beschrieben. Hierzu gehören beispielsweise das Vorhandensein von Redundanzen, die die Funktion ausfallender Komponenten übernehmen können, oder die Vorbereitung auf und der Umgang mit möglichen Stromausfällen. Auch wird diskutiert, ob die Dezentralisierung der Stromversorgung dazu beitragen kann, die Bewältigungskapazität zu erhöhen.

Um jedoch die Wechselwirkungen zwischen Bevölkerung und KRITIS bzw. die Folgen eines Stromausfalls für die Bevölkerung und weitere KRITIS einzubeziehen, bedarf es einer weiteren Betrachtung der Wirkungsketten, an deren Ausgangspunkt die Verwundbarkeit der Elektrizitätsversorgung steht. Im Verhältnis zur Verwundbarkeit der Stromversorgung selbst muss dabei die Abhängigkeit der Bevölkerung ebenso wie die Abhängigkeit anderer KRITIS berücksichtigt werden, um die gesamte Verwundbarkeit des Systems „KRITIS-Mensch“ in Bezug auf die Basisinfrastruktur Elektrizität zu verstehen. Diese Abhängigkeiten und ihre Bedeutung werden in Kapitel 5 beleuchtet. Eine entscheidende Rolle spielen dabei nicht nur Abhängigkeiten, sondern auch die Vernetzung des Gesamtsystems, die die Erfassung von Wirkfolgen erschwert. Kapitel 5.3 ist daher dem Stand der Forschung zur Erfassung der Komplexität gewidmet.

Nach der Analyse der Verwundbarkeit der Stromversorgung und der Auseinandersetzung mit den Folgen von Stromausfällen werden in Kapitel 6 Handlungsmöglichkeiten zum Umgang mit den verschiedenen Komponenten der Verwundbarkeit aufgezeigt. Hierzu gehören im Rahmen der Reduktion der Anfälligkeit insbesondere die Evaluierung möglicher neuer Normen, die Neuordnung der Organisationsstruktur und eine engere Kooperation der in der Elektrizitätserzeugung, -transformation und -distribution beteiligten Akteure. Auch stellen sich technische Fragen zur Reduktion der Anfälligkeit und Stärkung der Bewältigungskapazität, wie beispielswiese der Ausbau von Redundanzen oder die Entwicklung von Speichermöglichkeiten für Strom. Schließlich sind Übungen im Rahmen von Mitarbeiterschulungen und Einsätzen der Notfallkräfte wichtig, um angemessen auf einen Stromausfall reagieren zu können. Alle Maßnahmen können dabei im Rahmen von Risk Governance-Ansätzen aufgegriffen werden, die im letzten Teil (Kapitel 6.4) der Studie thematisiert werden.

Insgesamt gibt die Studie „State of the Art der Forschung zu Kritische Infrastrukturen am Beispiel Strom/ Stromausfall“ einen Überblick über derzeitige Erkenntnisse zur Verwundbarkeit Kritischer Elektrizitätsinfrastrukturen in den Bereichen Exposition,



Anfälligkeit und Bewältigungskapazität und zeigt erste Handlungsmöglichkeiten und präventive, sowie reaktive Lösungsansätze auf.





# 2 Die Entwicklung der Stromversorgung in Deutschland als Beispiel einer Kritischen Infrastruktur

Mit der Strommarktliberalisierung in Deutschland im Jahr 1998 und den daraus resultierenden Fusionen der großen Unternehmen kam es zu einer Konzentration auf der Erzeugungsebene, auf der sich die vier großen Verbundunternehmen EnBW, E.On, RWE und Vattenfall Europe im Laufe der Zeit etabliert haben. Zusammen verfügen sie über rund 80% der inländischen Stromerzeugungskapazitäten (BMU, 2006, S. 36). Abbildung 2 zeigt zudem die Regelzonen der vier großen Verbundunternehmen.

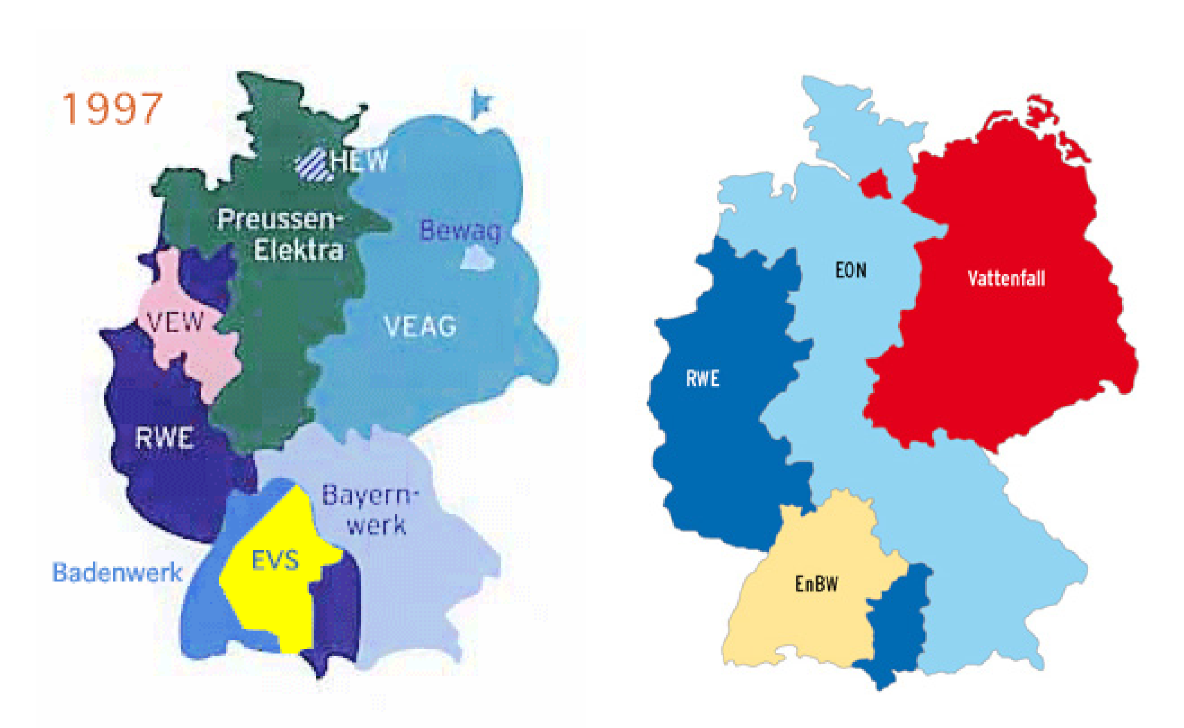



**Abbildung 2: Regelzonen Deutscher Übertragungsnetzbetreiber, 1997 und heute**

Quelle: (BMU, 2009; Leuschner, 2010)

Ingesamt findet die Stromversorgung auf drei Ebenen statt, auf denen insgesamt ca. 1.100 Unternehmen aktiv sind. Die vier Verbundunternehmen sind im Besitz des Übertragungsnetzes (Höchstspannungsnetz) zu deren Kunden Regional- und Lokalversorger, aber auch Geschäfts- und Privatabnehmer gehören. Auf der zweiten Stufe sind Regionalversorgungsunternehmen (REVU) mit einem Anteil von nur 8% an der gesamten Stromproduktion beteiligt. Der Strom – entweder von anderen Unternehmen erzeugt, oder selbst produziert – wird über die eigenen regionalen Verteilernetze an Lokalversorger oder Endkunden direkt veräußert. Auf der letzten Ebene werden die Endverbraucher direkt mit Strom, Wasser, Fernwärme und Gas über die



mehr als 900 Lokalversorgungsunternehmen (z.B. Stadtwerke) versorgt (BBK, 2005, S. 3).

Im Jahr 2009 wurden in Deutschland 597 Mrd. Kilowattstunden (kWh) Strom erzeugt. Grundlage der Stromerzeugung in Deutschland sind heute „vier Säulen“, bestehend aus Braunkohle (24%), Kernenergie (23%), Steinkohle (18%) und erneuerbare Energien (16%) (siehe Abbildung 3). Besonders durch den Ausbau von Windenergie in Deutschland konnte der Bereich der gesamten erneuerbaren Energien seit 2000 (6%) zunehmend an Bedeutung gewinnen (BMU, 2010, S. 9).

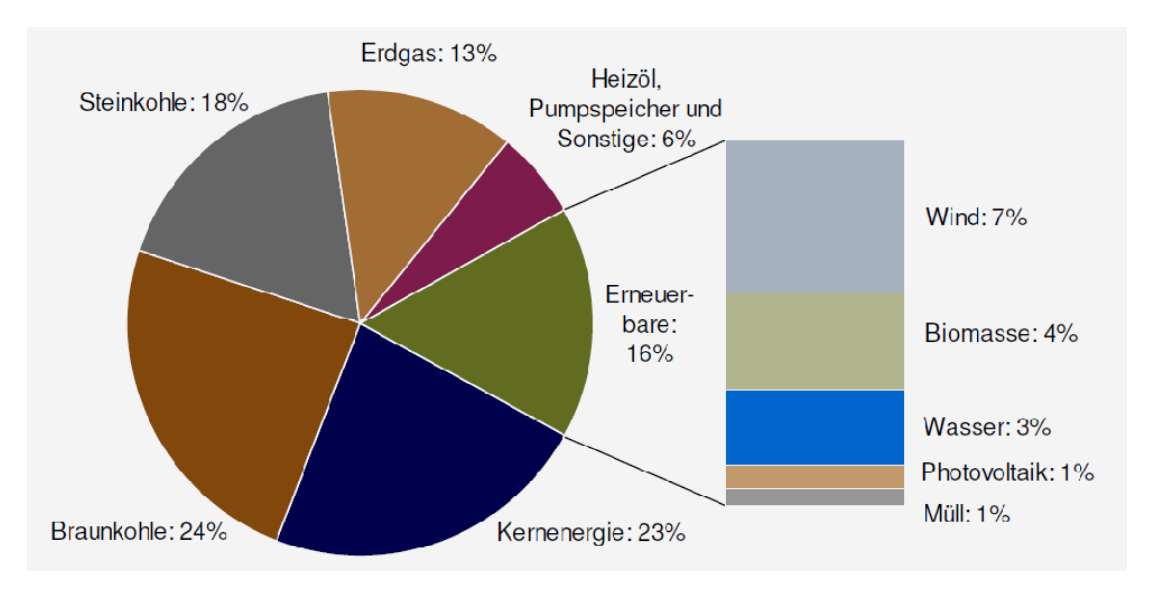



**Abbildung 3: Brutto Stromerzeugung nach Energieträgern in Deutschland 2009**

Quelle: (BDEW, 2010a, S. 1)

Der Grundlastbereich der deutschen Stromversorgung wird durch Kernenergie-, Braunkohle- und Wasserkraftwerke gedeckt, die rund um die Uhr laufen. Aus Kostengründen werden hingegen Steinkohle und Erdgas im Mittellastbereich eingesetzt. Besonders die Einspeisung der fluktuierenden Stromerzeugung aus Wind und Photovoltaik stellt das System vor eine Herausforderung für die zukünftige Versorgungssicherheit (BMU, 2006, S. 50).

Die Stromversorgung läuft über ein Stromnetz mit einer Gesamtlänge von über 1,7 Millionen Kilometer Leitungen. Je nach Zweck sind die Transportsysteme in vier Spannungsebenen gegliedert, die mit Wechselstrom betrieben werden und durch über 550.000 Transformatoren miteinander verbunden sind.

- Die **Höchstspannungsebene** (220.000 bis 380.000 Volt; 35.700 km Länge) dient in erster Linie zur überregionalen Verteilung des Stroms und zur Versorgung sehr großer Industriebetriebe. Zusätzlich bildet sie den Anschluss an die europäischen Netze.



- Die **Hochspannungsebene** operiert mit Spannungen von 60.000 bis 220.000 Volt und hat eine Länge von ca. 76.300 km. Sie beliefert lokale Stromversorger, größere Gewerbebetriebe, Industrieanlagen und die Eisenbahnen.
- Die **Mittelspannungsebene** (1.000 bis 60.000 Volt; 507.200 km Länge) beliefert u. a. lokale Verteilernetze sowie kleinere und mittlere Betriebe in der Industrie und im Gewerbe.
- Die **Niederspannungsebene** liefert schließlich den Strom mit der bekannten Spannung von 230 Volt oder 400 Volt an die Endverbraucher wie z.B. die Haushalte, kleinere Gewerbeunternehmen und landwirtschaftliche Betriebe. Die Länge dieses Netzes beträgt ca. 1.160.000 km. (BDEW, 2010b, S. 2)

Grundsätzlich muss bei der Stromversorgung zwischen Komponenten und Prozessen auf den verschiedenen Ebenen unterschieden werden. Dies ist speziell für die spätere Untersuchung von Exposition, Anfälligkeit und Bewältigungskapazität von großer Bedeutung. Als Komponenten werden

- Kraftwerke,
- Umspannwerke/Transformatoren,
- Netzleitstellen,
- Kabelverteilerkasten,
- Höchst-, Hoch-, Mittel- und Niederspannungsleitungen

bezeichnet. Die Prozesse dagegen sind Abläufe, die in den jeweiligen Komponenten eine Rolle spielen. Kraftwerke erzeugen den Strom, der von Umspannwerken auf die jeweils untere Spannungsebene transformiert wird. Netzleitstellen überwachen und steuern das Netz, sodass der Strom über die Kabelverteilerkasten an den einzelnen Abnehmer geliefert werden kann. Die Verbindungskomponenten zwischen den verschiedenen Spannungsebenen sind die Leitungen, die den Strom (je nach Spannung) transportieren. Abbildung 4 liefert einen groben Überblick über die Verbindungen der unterschiedlichen Spannungsebenen, deren Komponenten sowie die Endabnehmer (Krings, in Druck, S. 29).



**Abbildung 4: Stromnetz in Europa im 20. Jahrhundert**

Quelle: (Riepl, 2010)

Um eine gewisse Sicherheit gegenüber Stromausfällen zu gewährleisten, werden Übertragungsnetze durch das sogenannte (n-1)-Kriterium geplant. Das heißt, ein beliebiger der insgesamt n Versorgungswege kann störungsbedingt ausfallen, ohne dass dadurch andere Betriebsmittel unzulässig belastet werden oder sich deren Spannung zu stark verändert. Dieses Kriterium sichert somit die für hohe Versorgungssicherheit notwendige Redundanz (Oswald, o.J., S. 5). In der Praxis sind daher Strommasten so konzipiert, dass auf beiden Seiten des Mastes sechs Leitungen hängen. Einen gemeinsamen Stromkreis stellen dabei jeweils drei Leitungen her. Bei einem Ausfall eines Stromkreises kann die Versorgung somit durch den anderen Stromkreis



kompensiert beziehungsweise aufgefangen werden[4] (RWE, 2006; Brakelmann, 2006, S. 2). Trotzdem kann es in einem (n-1)-sicheren Netz zu kurzzeitigen Versorgungsunterbrechungen des Systems kommen. Diese Anfälligkeit des Versorgungssystems wird in Kapitel 4.2 näher behandelt und untersucht.

Abschließend fasst die folgende Tabelle die Funktionen der Spannungsnetze auf den oben erwähnten Ebenen noch einmal zusammen.

**Tabelle 1: Elemente der öffentlichen Stromversorgung[5]**

| Anlagen | Funktion | Bemerkungen |
|---|---|---|
| Kraftwerke | Stromerzeugung aus nuklearen, fossilen oder regenerativen Energiequellen | Je nach Einsatzbereich wird zwischen Grund-, Mittel- und Spitzenlastkraftwerken bzw. Regelkraftwerken unterschieden. |
| Übertragungsnetz (380 bzw. 220 kV) | - Großräumiger Stromtransport<br>- Ausgleich von Leistungsschwankungen und Transport von Regelenergie im europäischen Verbundbetrieb | - Auslegung nach dem (n-1)-Kriterium, d. h. Ausfall einer einzelnen Netzkomponente führt nicht zu einer unzulässigen Überschreitung von Betriebsparametern bzw. zur Versorgungsunterbrechung<br>- fast ausschließlich Freileitungen |
| Überregionales Verteilnetz (110 kV) | Stromverteilung im überregionalen Bereich | - Auslegung nach dem (n-1)-Kriterium<br>- meist Freileitungen |
| Regionale Verteil- und Ortsnetze (30, 20, 10 kV sowie 400/230V) | Stromverteilung im<br>- regionalen Bereich<br>- Ortsbereich von Städten, Gemeinden und auf dem Lande | - (n-1)-Kriterium in der Regel nicht erfüllt, d. h. Ausfall einzelner Komponenten führt meist zu Versorgungsunterbrechung<br>- häufig Erdkabelleitungen |
| Netzführungssysteme | - Steuerung und Überwachung der Netze<br>- Unterstützung von Entstörmaßnahmen | Systeme sind redundant ausgelegt und durch USV- und Notstromanlagen sehr gut abgesichert |

Quelle: (Hiete et al., 2010)

[4] Das deutsche Stromnetz wird in diesem Zusammenhang auch als engmaschig beschrieben (Kuhn, 2005, S. 34 f)

[5] Die in der Tabelle bezeichneten *Anlagen* können auch, als die im Verlauf der Studie häufig erwähnten, Komponenten verstanden werden; die *Funktionen* entsprechen den Prozessen.





# 3 Das Konzept der Verwundbarkeit

Ein klares Verständnis des Begriffs *Verwundbarkeit* sowie der unterschiedlichen Vulnerabilitätskonzepte ist Voraussetzung für die Analyse der Verwundbarkeit der Elektrizitätsversorgung und der damit einhergehenden Maßnahmen diese zu reduzieren. Bevor jedoch zwei im Kontext dieser Studie relevante Konzepte näher vorgestellt, sowie kritisch untersucht werden, soll ein Definitionsexkurs die Vielschichtigkeit der Verwundbarkeitsforschung und ihrer unterschiedlichen Denkschulen aufzeigen. Aus diesem Grund werden im Folgenden Kapitel der Begriff *Vulnerabilität* und mögliche Konzepte zur Erfassung vorgestellt.

## 3.1 Definitionen

Der Begriff der Vulnerabilität leitet sich aus dem lateinischen Verb *vulnerare* (verwunden, verletzen*)* ab, der mit dem Begriff der Verwundbarkeit synonym verwendet wird. Sowohl die wissenschaftlichen Konzepte als auch die Definitionen gehen jedoch über die wörtliche Bedeutung hinaus (Lenz, 2009, S. 29). Der Begriff der Vulnerabilität und seine Konzeption werden, je nach naturwissenschaftlichem oder sozialwissenschaftlichem Fokus, in der Vulnerabilitätsforschung sehr unterschiedlich definiert. So wird oftmals zwischen sozialer und biophysischer Verwundbarkeit unterschieden. Während der Ansatz der biophysischen Verwundbarkeit eher eine Empfindlichkeit vorher definierter Risikoelemente gegenüber einer Naturgefahr beschreibt (Bohle & Glade, 2008, S. 99) – beispielsweise Ökosystemdegradierung – bezieht sich die soziale Verwundbarkeit auf gesellschaftliche Zustände und deren Fähigkeit, Ereignisse mit Hilfe verschiedener Strategien zu bewältigen (Villagrán de León, 2006, S. 14). Dennoch beinhaltet soziale Verwundbarkeit weit mehr Aspekte als nur die demographischen Merkmale, wie beispielsweise Geschlecht, Alter oder Einkommen. Soziale Verwundbarkeit bezieht sich ebenso auf ökonomische und ökologische Aspekte, die eng mit der sozialen Verwundbarkeit verknüpft sind (Birkmann, 2006, S. 14).

Entsprechend vielfältig sind die Definitionen und Untersuchungsansätze, deren vollständige Auflistung jedoch hier nicht vorgenommen wird. An dieser Stelle kann auf entsprechende Übersichten u.a. bei Thywissen (2006) oder vergleichende Betrachtungen unterschiedlicher Denkschulen verwiesen werden (Bohle & Glade, 2008; Turner, et al., 2003; Birkmann, 2006; Villagrán de León, 2006).

In der vorliegenden Studie werden unterschiedliche Denkschulen zusammengeführt, wobei insbesondere auf die weltweit verbreitete Definition von Vulnerabilität der Internationalen Strategie für Katastrophenreduzierung UN/ISDR (United Nations



International Strategy for Disaster Reduction) Bezug genommen wird. UN/ISDR definiert Verwundbarkeit wie folgt:

> *"The conditions determined by physical, social, economic and environmental factors or processes, which increase the susceptibility of a community to the impact of hazards."* (UN/ISDR, 2004, S. 7)

Sinngemäß übersetzt beinhaltet Verwundbarkeit Zustände und Prozesse, die durch physische, soziale, ökonomische und ökologische Faktoren bestimmt werden und die Schadensanfälligkeit einer Gemeinschaft bzw. Gesellschaft gegenüber den Einwirkungen einer Gefahr erhöhen. Diese Definition folgt eher einem sozialwissenschaftlichen Ansatz, wobei insbesondere der multi-disziplinäre Charakter der Vulnerabilität betont wird.

Trotz unterschiedlicher Ansätze und Definitionen von Verwundbarkeit sollte berücksichtigt werden, dass Vulnerabilität nicht nur eine Bewertung direkter Einflüsse von Gefahren darstellt. Vielmehr müssen auch die Fähigkeiten der Gesellschaft, die Einflüsse gefährlicher Ereignisse zu bewältigen bzw. die negativen Auswirkungen auszuhalten, einbezogen werden (vgl. Birkmann, 2006; Wisner, 2004). Laut Birkmann (2006) ist die Verwundbarkeit nur zum Teil durch die Art der Gefahr festgelegt. Vielmehr ist sie durch unsichere Lebensgrundlagen, den Grad des Selbstschutzes oder des sozialen Schutzes sowie institutionelle Gegebenheiten, beeinflusst (Birkmann, 2006, S. 13 f).

## 3.2 Konzepte der Verwundbarkeit

Um die genannte Definition von Verwundbarkeit in einen konzeptionellen Rahmen zu übertragen, werden im Folgenden zwei der gängigen Verwundbarkeitskonzepte näher vorgestellt und untersucht. Bevor jedoch auf deren Struktur und Aufbau eingegangen wird, sollen zunächst deren Schlüsselbegriffe *Exposition, Resilienz, Anfälligkeit, Bewältigungskapazität und Risiko* kurz erläutert werden:

Exposition wird unter anderem folgendermaßen beschrieben:

> *"Elements at risk, an inventory of those people or artefacts that are exposed to a hazard."* (UNDP, 2004, S. 98)

Sinngemäß übersetzt beschreibt Exposition Risikoelemente (Menschen oder Gegenstände), die einer Gefahr gegenüber räumlich und zeitlich ausgesetzt sind (Cardona, 2006). Nach Birkmann (2006) ist es besonders wichtig zu beachten, dass ein Element oder System nur dann gefährdet ist, wenn es exponiert und verwundbar gegenüber einem möglichen Naturereignis ist. Der Begriff der Resilienz wird demgegenüber nach dem Ansatz von Turner et al. (2003) als Fähigkeit verstanden



bestimmte zentrale Funktionen und Systemzustände auch während und nach dem Einfluss von Gefahren und Stressoren aufrechtzuerhalten oder diese schnell wieder herzustellen. In diesem Kontext wird der Begriff Resilienz wie folgt definiert:

> *“The concept [of resilience] has been used to characterize a system’s ability to bounce back to a reference state after a disturbance and the capacity of a system to maintain certain structures and functions despite disturbance.”* (Turner et al., 2003, S. 8075)

Im Vergleich zum Begriff Resilienz, der positive Eigenschaften eines Systems in den Vordergrund stellt, wird mit dem Begriff der Anfälligkeit oder Fragilität versucht, Defizite und mögliche Schwachpunkte in einem System oder Subjekt/Objekt zu charakterisieren. In diesem Kontext kann Anfälligkeit folgendermaßen definiert werden:

> *“Susceptibility means that an exposed system – regardless of whether it reacts rapidly or slowly – can face serious harm and disruption or is adversely affected.”* (Birkmann et al., 2009, S. 54)

Sinngemäß übersetzt bedeutet Anfälligkeit, dass ein exponiertes System oder Element auch im Falle des Eintritts eines Ereignisses fragil und schadensanfällig ist, d.h. auch ein höheres Maß an Schäden und Problemen in der Erholung nach dem Ereignis aufweist, als ein System das zwar exponiert jedoch nur wenig anfällig gegenüber den Einwirkungen des Ereignisses ist.

Von grundlegender Bedeutung für die Definition von Verwundbarkeit sowie Ansätze der Verwundbarkeitsforschung – wie beispielsweise das *BBC-Rahmenkonzept* oder das *Gekoppelte Mensch-Umwelt-System* – ist zudem der Begriff Bewältigungskapazität (Coping Capacity), der sich mit den Kapazitäten und Bewältigungsmöglichkeiten vulnerabler Systeme befasst (UN/ISDR, 2009; Pelling, 2005, S. 146). Die United Nations International Strategy for Disaster Reduction (UN/ISDR) definiert Capacity als:

> *“A combination of all the strengths and resources available within a community, society or organization that can reduce the level of risk, or the effects of a disaster.”* (UN/ISDR, 2004, S. 2)

und Bewältigungskapazität wie folgt:

> *“The means by which people or organizations use available resources and abilities to face adverse consequences that could lead to a disaster.”* (UN/ISDR, 2004, S. 2)

Sinngemäß bezeichnet Capacity die gesamten zur Verfügung stehenden Möglichkeiten und Ressourcen innerhalb einer Gemeinschaft bzw. Gesellschaft, das Risiko oder die Auswirkungen einer Krise oder Katastrophe zu reduzieren. Bewältigungskapazität



bezeichnet demzufolge das Anwenden der vorhandenen Möglichkeiten und Ressourcen, um den negativen Auswirkungen [eines Ereignisses] entgegenzuwirken, die zu einer Katastrophe führen könnten.

Ein im Zusammenhang der Verwundbarkeitsforschung zentraler Begriff ist Risiko. Laut UN/ISDR wird Risiko definiert als die Kombination der Wahrscheinlichkeit des Auftretens einer Gefahr und seiner negativen Auswirkungen (UN/ISDR, 2009). Da die negativen Auswirkungen durch die Verwundbarkeit eines Systems bestimmt werden, kann das Risiko in folgender Formel beschrieben werden:

| Risiko = f (Gefahr, Verwundbarkeit) |
|---|

Das Risikoverständnis ist besonders im Hinblick auf mögliche Handlungsoptionen von besonderer Bedeutung und wird in Kapitel 6.4 aufgegriffen und näher behandelt. Nachdem die wesentlichen Begriffe der folgenden Konzepte definiert und abgegrenzt wurden, folgt in den nächsten beiden Abschnitten die Auseinandersetzung mit zwei in der Verwundbarkeitsforschung gängigen Rahmenkonzepten, sogenannten Frameworks.

### 3.2.1 Das BBC-Framework

Das BBC-Rahmenkonzept, welches auf Arbeiten von Bogardi, Birkmann und Cardona basiert, verbindet Elemente aus verschiedenen Ansätzen der Verwundbarkeitsforschung und versucht insbesondere die Verwundbarkeitsabschätzung mit dem Konzept der nachhaltigen Entwicklung zu verbinden (vgl. Birkmann, 2006). Von zentraler Bedeutung ist das Rückkopplungssystem bestehend aus dem Zusammenspiel von Exposition, Anfälligkeit und Bewältigungskapazität einerseits, sowie den unterschiedlichen Maßnahmen zur Reduzierung von Verwundbarkeit andererseits. Definiert wird Vulnerabilität in diesem Rahmenkonzept zum einen durch exponierte und anfällige Elemente, zum anderen durch die Bewältigungskapazität der betroffenen Objekte (beispielsweise soziale Gruppen) (Anwar et al., 2008, S. 3). Diese Komponenten stehen im Mittelpunkt des Modells (siehe Abbildung 5). Im Vergleich zu anderen Konzepten wird Verwundbarkeit nicht nur als Ausmaß der Zerstörung (statischer Zustand) sondern vielmehr als ein *dynamischer* Prozess betrachtet, der sich durch Rückkopplungsmechanismen auszeichnet.

> *„Da die sozialen Beziehungen und Aktivitäten verwundbarer Gruppen, die gesellschaftlichen Prozesse, in die sie eingebettet sind und auch die Naturgefahren, denen sie ausgesetzt sind, von hoher Dynamik sind, ist Verwundbarkeit stets als ein dynamisches Konzept zu begreifen."* (Bohle & Glade, 2008, S. 103)



Beispielsweise steigt die Verwundbarkeit einer Gesellschaft, wenn ihre Armut durch eine Katastrophe vergrößert wurde, sodass die nächste Katastrophe noch zerstörerischere Auswirkungen hat. Im Umkehrschluss kann jedoch ein vergleichsweise kleines Ereignis das Bewusstsein der Gesellschaft schärfen und somit deren Verwundbarkeit durch Schutzmaßnahmen reduzieren. Verwundbarkeit wird in diesem Konzept ebenso als ein *mehrdimensionaler* Prozess beschrieben, der sich im Wesentlichen in drei Sphären (Umweltsphäre, soziale und ökonomische Sphäre) abspielt, die gleichzeitig sehr stark miteinander interagieren (Birkmann, 2006, S. 13).

Zudem bezieht sich Verwundbarkeit immer auf ein Risikoelement (Objekt) sowie seine spezifischen räumlichen und strukturellen Ausprägungen. Diese Objekte oder Subjekte können sowohl Infrastruktursysteme als auch Menschen, Sachgüter, oder räumliche Einheiten (z.B. Bundesländer) sein. Neben dem O*bjektbezug* ist Verwundbarkeit auch *gefahrenspezifisch*, das heißt, sie wird erst durch das Eintreten eines Ereignisses und die daraus resultierende Gefahr deutlich und äußert sich beispielsweise in konkreten monetären oder physischen Schäden.

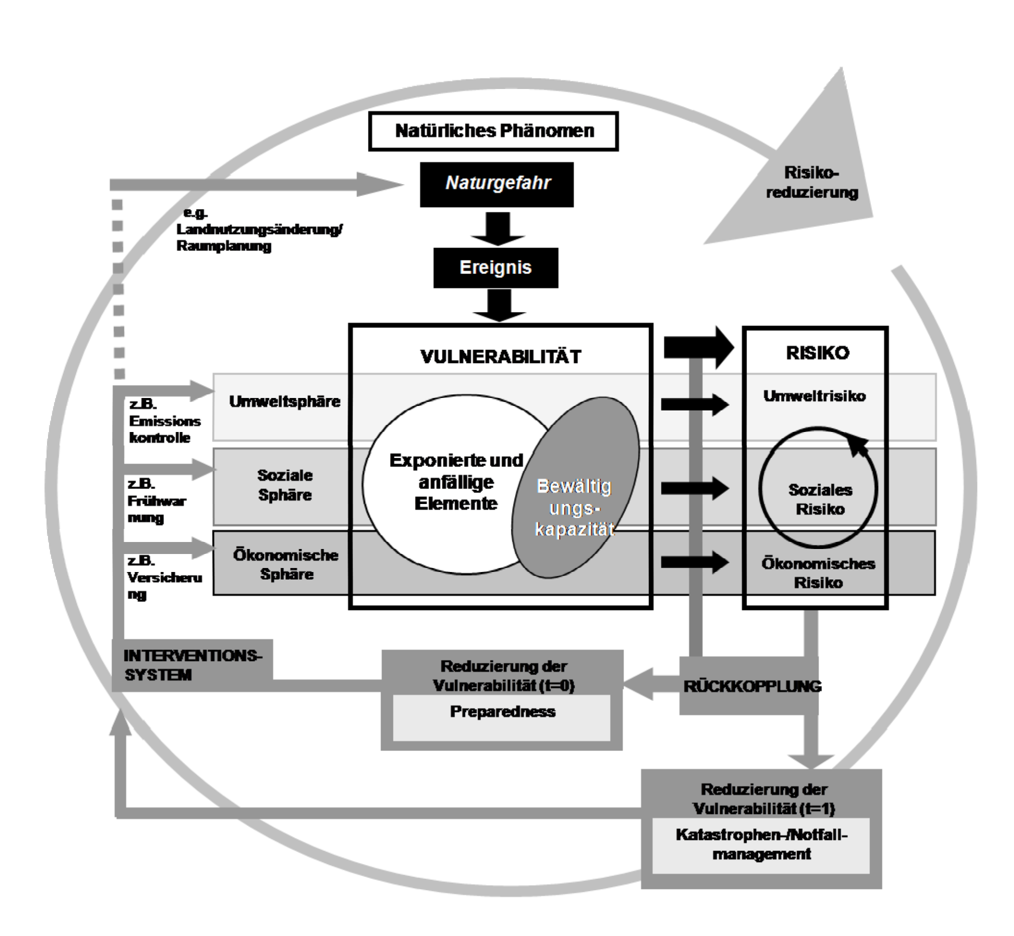



**Abbildung 5: BBC Rahmenkonzept**

Quelle: (Birkmann, 2006, S. 34, übersetzt)



Die Reduzierung der Verwundbarkeit kann im Rahmen eines Rückkopplungsprozesses in zwei unterschiedliche Kategorien unterteilt werden: Einerseits handelt es sich um Präventivmaßnahmen bevor Ereignisse/Katastrophen eintreten (t=0) und andererseits um notwendige Handlungen im Katastrophenfall (t=1). Folglich steht während einer Katastrophe das Katastrophenmanagement bzw. die Katastrophenhilfe im Vordergrund. Im Vorfeld einer Katastrophe stellen die Bereitschaft und Vorbereitung einen wesentlichen Faktor zur Reduzierung der Verwundbarkeit dar. Diese Unterteilung in zwei Zeitperioden macht deutlich, dass schon vor dem Eintritt eines Ereignisses Maßnahmen zur Reduzierung der Verwundbarkeit getroffen werden können, um Ereignisse nicht zu Katastrophen werden zu lassen. Eine Verbesserung des Katastrophen- und Notfallmanagements ist zwar im Hinblick auf ein schnelleres und sichereres Eingreifen von großer Bedeutung, doch wesentlich wichtiger – besonders auf politischer Entscheidungsebene – sind vorausschauende und nachhaltige Maßnahmen zur Reduzierung der Verwundbarkeit innerhalb der drei Sphären (*preparedness*) (Birkmann, 2006, S. 36).

Ein weiteres Element des Rahmenkonzeptes ist das Risiko, welches als Ergebnis aus der Interaktion eines Naturereignisses und der existierenden Verwundbarkeit betrachtet wird. Dieses Grundverständnis greift die Definition von Risiko im Kontext der Naturgefahrenforschung auf (vgl. UN/ISDR, 2004). Risiko wird hier nicht weiter in hohes bzw. niedriges Risiko klassifiziert, jedoch auf die drei Sphären (sozial, ökologisch und ökonomisch) bezogen, die den thematischen Rahmen, in dem Verwundbarkeit gemessen werden soll, festlegen. Die soziale wie die ökonomische Sphäre sind von etwas größerer Bedeutung, doch die Eingliederung der Umweltsphäre ist unbedingt notwendig und zeigt den engen Zusammenhang zwischen Natur und Gesellschaft. Die drei genannten Sphären sind sehr eng miteinander verbunden, interagieren miteinander und können daher nicht isoliert voneinander betrachtet werden (Birkmann, 2006, S. 35).

Basis des Konzeptes ist das Verständnis, dass sich Verwundbarkeit aus den Komponenten Exposition, Anfälligkeit und Bewältigungskapazität zusammensetzt:

| f (Vulnerabilität) = Exposition (Hazard), Anfälligkeit, Bewältigungskapazität |
|---|

### 3.2.2 Verwundbarkeitsmodell für gekoppelte Mensch-Umwelt-Systeme nach Turner

Das gekoppelte Mensch-Umwelt-System von Turner et al. (2003), das in Abbildung 6 dargestellt ist, verbindet die sozialwissenschaftliche mit der naturwissenschaftlichen Verwundbarkeitsforschung in einem mehrdimensionalen, komplexen Modell. Das Konzept basiert im Wesentlichen auf drei wichtigen Komponenten, die auf unterschiedlichen Ebenen miteinander interagieren:



(i) Die natürlichen (unterer Teil) und gesellschaftlichen (oberer Teil) Zustände und Prozesse, die von außen in das System einwirken,

(ii) Störungen und Stressfaktoren, die sich aus den Veränderungen dieser Zustände und Prozesse entwickeln, sowie

(iii) Rückkopplungseffekte zwischen den Komponenten des sozio-ökologischen Systems und zwischen den verschiedenen Ebenen von Verwundbarkeit – global bis lokal.

Verwundbarkeit selbst wird in diesem Modell als Funktion von Exposition, Anfälligkeit und Resilienz (Widerstandsfähigkeit) aufgefasst und beinhaltet zudem Bewältigung, Ereignis, Anpassung und Reaktion. Somit ist Vulnerabilität hier im Vergleich zum BBC-Framework sehr viel weiter gefasst. Eine Besonderheit ist dabei die Berücksichtigung sozial-ökologischer Interaktionen im Rahmen der Anfälligkeit (Birkmann, 2006, S. 27; Bohle & Glade, 2008, S. 109 f; Turner et al., 2003, S. 8076 f).

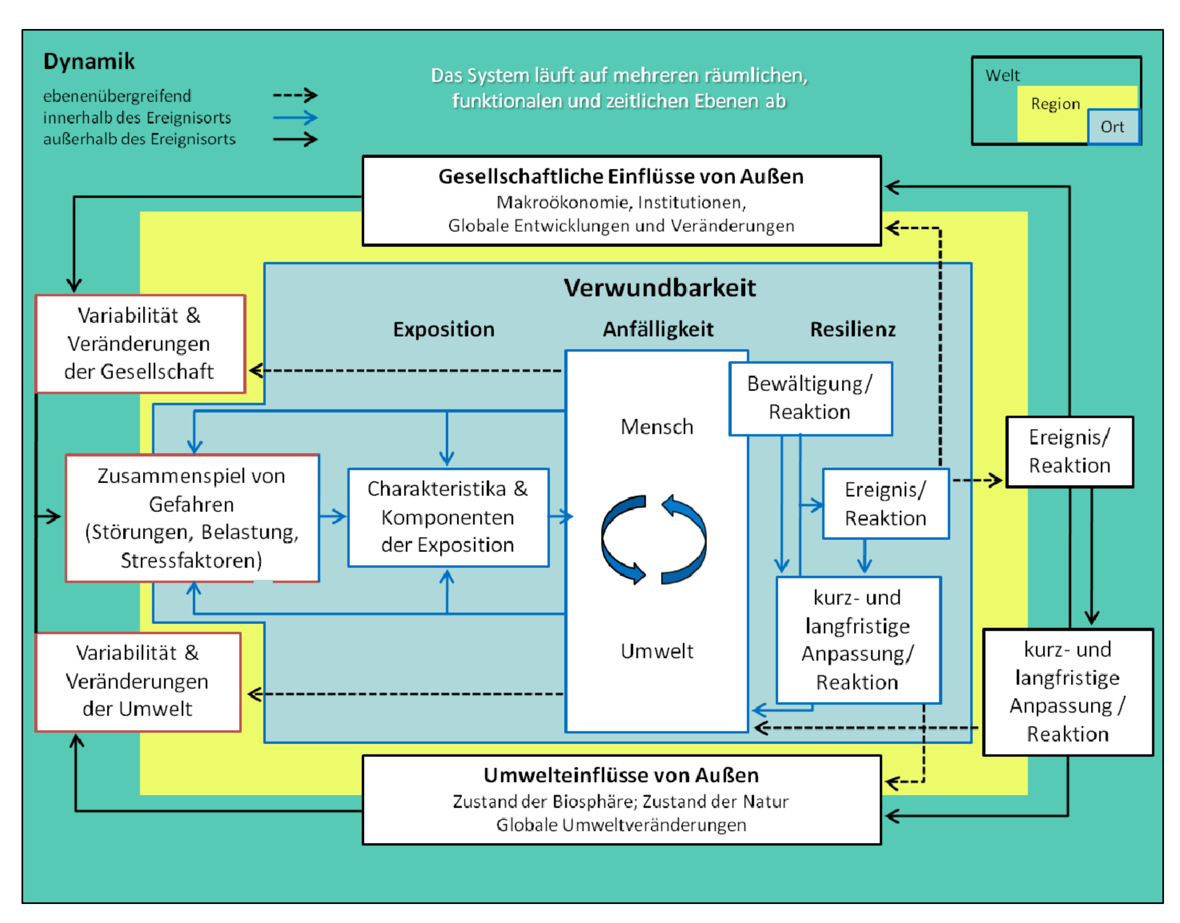



**Abbildung 6: Gekoppeltes Mensch-Umwelt-System nach Turner**

Quelle: (Turner et al., 2003, S. 8076, übersetzt)



Das gekoppelte Mensch-Umwelt-System als Zentrum bzw. Schlüsselkomponente des Modells legt zunächst, ungeachtet der räumlichen Dimension, die Ebene der Analyse fest. Die Ausprägung der Gefahren, die sowohl außerhalb als auch innerhalb des Systems entstehen können, ist einerseits abhängig von diesem gekoppelten System, andererseits wird sie durch die Veränderungen der natürlichen und gesellschaftlichen Zustände beeinflusst. Zusätzlich legt das Mensch-Umwelt-System seine Anfälligkeit gegenüber jeglicher Exposition fest. Die Interaktion der sozialen und ökologischen Zustände wirkt sich zudem auch auf die Bewältigungs- und Reaktionsstrategien infolge von Gefahren bzw. Störungen aus. Diese Strategien befinden sich wiederum ständig in einem Veränderungsprozess, besonders vorangetrieben durch Erfahrungswerte früherer Ereignisse. Eine weitere Rückkopplung besteht zwischen den sozialen und ökologischen Reaktions- und Bewältigungsmechanismen, die sich gegenseitig beeinflussen, sodass eine Reaktion im sozialen System zu einer verbesserten oder verschlechterten Bewältigungsfähigkeit im ökologischen System führen kann und umgekehrt. Reaktionen, Bewältigungsmechanismen und Anpassungsstrategien können sowohl individueller/unabhängiger als auch politischer/institutioneller Art sein und haben Auswirkungen auf die Resilienz der Gesellschaft bzw. des Systems (Turner et al., 2003, S. 8077).

Sehr deutlich wird in diesem Framework, wie komplex, interaktiv und mehrdimensional die Verwundbarkeit ist und wie sehr sie auf unterschiedlichste Art und Weise von außen sowie von innen beeinflusst wird (Turner et al., 2003, S. 8077).

Zusammenfassend kann somit festgehalten werden, dass zwar verschiedene Ansätze zur Konzeptualisierung der Verwundbarkeit bestehen, diese jedoch in der Berücksichtigung der Komponenten *Exposition*, *Anfälligkeit* und *Bewältigungskapazität* übereinstimmen.

## 3.3 Konzepte zur Verwundbarkeit Kritischer Infrastrukturen

Neben der Systematisierung und konzeptionellen Weiterentwicklung des Ansatzes der Vulnerabilität bzw. Verwundbarkeit, ist auch die Erfassung und Messung von Verwundbarkeit eine der zentralen Fragestellungen in der Vulnerabilitätsforschung. Wer die Zusammenhänge versteht, die Störungen oder Ausfälle beeinflussen, kann Maßnahmen bezüglich Planung, Management und Handhabung von Elektrizitätssystemen entwickeln, um Störungen oder Ausfälle zu verhindern bzw. deren Auswirkungen zu verringern (Holmgren & Molin, 2006, S. 243).

Betrachtet man das Konzept der Vulnerabilität im Zusammenhang mit Kritischer Infrastruktur, so muss Vulnerabilität zunächst in diesem Kontext weiter konkretisiert bzw. definiert werden. In diesem Zusammenhang definiert Lenz (2009) Vulnerabilität als *„die gefahrenspezifische Anfälligkeit einer Kritischen Infrastruktur für Beeinträchtigung oder Ausfall ihrer Funktionsfähigkeit, welche zur Unterbrechung der*



*Versorgung der Bevölkerung mit wichtigen Gütern und Diensten führen können.“* (Lenz, 2009, S. 30)

Grundsätzlich muss bei der Analyse berücksichtigt werden, dass die Verwundbarkeit eines Elements standortbezogen ist und sich mit der räumlichen Skala verändert. Demzufolge wird die Vulnerabilität einzelner Infrastrukturelemente im Vergleich zur Gesamtinfrastruktur je nach Betrachtungsebene von unterschiedlichen Einflussfaktoren bestimmt. Für die Analyse der KRITIS-Sektoren ist daher beispielsweise die nationale Betrachtungsebene sinnvoll, untersucht man einzelne Infrastrukturen ist eher die regionale Ebene zu empfehlen und bei speziellen Infrastrukturelementen die lokale Ebene (Lenz, 2009, S. 35). Im folgenden Kapitel werden verschiedene Ansätze zur Bemessung von Verwundbarkeit Kritischer Infrastrukturen und im Speziellen der Kritischen Elektrizitätsinfrastruktur aufgezeigt.

### 3.3.1 Verwundbarkeitsbemessung nach Holmgren

Aus den Erfahrungen und Ergebnissen einer Systemstudie der *Swedish Defence Research Agency (FOI)* und basierend auf Analysen von Einarsson und Rausand (1998) hat Holmgren (2007) ein Konzept zur Verwundbarkeitsbemessung entwickelt. Grundsätzlich argumentiert Holmgren, dass Störungen in der Energieversorgung unterschiedliche Ursachen haben können. Dabei handelt es sich entweder um natürliche Einflüsse, menschliches bzw. technisches Versagen oder kriminelle Handlungen – Sabotage oder terroristische Anschläge. Eines dieser Ereignisse löst eine Reaktion im System aus, die mehr oder weniger schwere Folgen für Teile der Gesellschaft haben kann. Dabei sind die Folgen und Auswirkungen eines Ausfalls von verschiedenen Faktoren, wie betroffener Region, Dauer des Ausfalls, Zeitpunkt, Wetterbedingungen, usw. abhängig (Holmgren, 2007). Neben der Gefahr als Auslöser, wird jedoch auch im technischen Zusammenhang deutlich, dass es sowohl Komponenten, die die Verwundbarkeit negativ beeinflussen (Anfälligkeit), auch Faktoren gibt, die die Fähigkeit des Systems fördern, seine Funktionsfähigkeit während solcher Einwirkungen von Störungen aufrecht zu erhalten (Holmgren, 2007). Diese Differenzierung trägt den vorher skizzierten Ansätzen zur Unterscheidung zwischen Anfälligkeit und Bewältigungskapazität Rechnung.

Zur Analyse der Verwundbarkeit des Systems schlägt Holmgren (2007) verschiedene Methoden vor, die je nach Datengrundlage die Wahrscheinlichkeit negativer Auswirkungen für die Gesellschaft/das System abschätzen.

- Statistische Analyse empirischer Daten über Störungen bzw. Ausfälle
- Mathematische Modellierung verbunden mit empirischen Daten
- Expertenbeurteilungen



Von diesen Methoden scheint die statistische Analyse in dem Maße sinnvoll, als dass sie eine differenzierte Analyse über die Hazards/Gefahren, also die Auslöser, der Vergangenheit ermöglicht, aus denen für die Zukunft gelernt werden kann (siehe hierzu auch Kapitel 5.4). Grundlage dieser Methode sind Daten über Störungen und Ausfälle der Vergangenheit, die je nach Ursache, Häufigkeit und Auswirkungen (Länge des Stromausfalls in Megawattstunde (MWh)) gegliedert sind. Demzufolge werden in dieser Art der Verwundbarkeitsabschätzung äußere Faktoren und deren Folgen in die Bemessung einbezogen. Spieltheoretische Ansätze und mathematische Rechnungen hingegen mögen zwar Auskunft über systeminterne Schwachstellen oder das mögliche Auftreten von Fehlern geben. Jedoch fehlen diesen Ansätzen eine umfassende Betrachtung verschiedener Gefahren und deren Ursachen sowie deren Folgen für die Bevölkerung. In Verbindung mit statistischen Analysen können beispielsweise Expertenbeurteilungen den Ergebnissen zusätzlich Aussagekraft verleihen und politische Handlungsmöglichkeiten aufzeigen. Besonders die Interaktionen und Abhängigkeiten des Systems Kritischer Infrastrukturen verlangen daher eine Kombination der verschiedenen Ansätze (Holmgren & Molin, 2006, S. 244). Eine wichtige Herausforderung für Analysen der Verwundbarkeit Kritischer Infrastrukturen ist die Datenbeschaffung, da es beim Informationsaustausch zwischen den oftmals privaten Betreibern und den öffentlichen Institutionen häufig zu Schwierigkeiten kommt bzw. der Grad vorliegender und leicht erhältlicher Informationen vielfach gering ist (Rinaldi, 2004, S. 7; Holmgren, 2007, S. 36).

Laut Holmgren (2007) sind die Ergebnisse der Verwundbarkeitsanalyse eines Infrastruktursystems aus verschiedenen Gründen hilfreich. Einerseits können Ereignisse bzw. Gefahren, die zu negativen Konsequenzen führen, im Voraus identifiziert und somit gleichzeitig Schwachstellen des Systems offengelegt werden. Andererseits hilft eine derartige Analyse die Abläufe des Systems zu verstehen und bietet Möglichkeiten die Belastbarkeit und Widerstandskraft durch Handlungsmaßnahmen zu erhöhen. Dies stärkt gleichzeitig das Bewusstsein von Risiko, sodass neue Reaktionsmöglichkeiten in potentiellen Krisensituationen entwickelt werden können und die Verwundbarkeit reduziert werden kann (Holmgren, 2007, S. 35 f; Rinaldi, 2004, S. 4).

### 3.3.2 Verwundbarkeitsanalyse nach Krings

Im Zusammenhang des Projekts „Indikatoren zur Abschätzung von Vulnerabilität und Bewältigungspotenzialen am Beispiel von wasserbezogenen Naturgefahren in urbanen Räumen“, welches durch das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) gefördert wurde, ist eine Methodik zur Vulnerabilitätsabschätzung entwickelt worden, die verschiedene Phasen und Schritte zur Abschätzung der Verwundbarkeit der Elektrizitätsversorgung systematisch darstellt. Das in Abbildung 7 dargestellte Konzept von Krings (in Druck), basiert auf dem Verständnis der Verwundbarkeit als Funktion



aus *Exposition, Anfälligkeit* und *Bewältigungskapazität* (siehe detailliertere Erläuterungen der Begriffe in 3.2).

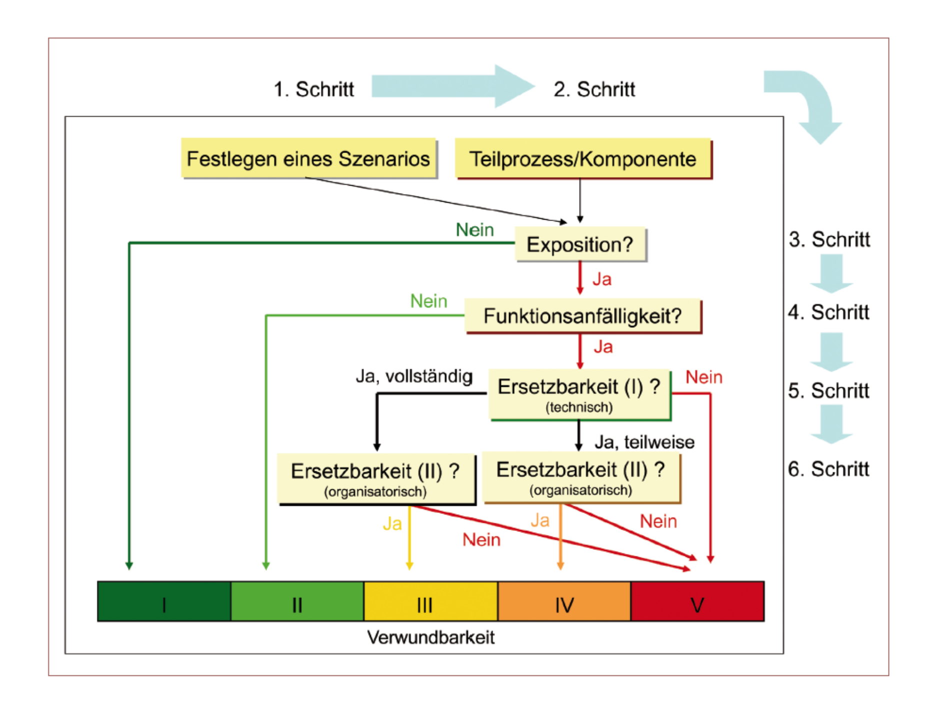



**Abbildung 7: Schematische Darstellung zur Erfassung der Verwundbarkeit von KRITIS-Komponenten**

Quelle: (Krings, in Druck, S. 25)

Anhand des in Abbildung 7 dargestellten Konzeptes ist die Einschätzung der Vulnerabilität einzelner Komponenten der Stromversorgung möglich. Je nachdem, ob eine Komponente gegenüber einer bestimmten Gefahr exponiert ist, kann überprüft werden, ob sie in diesem Falle funktionsanfällig (4. Schritt) und ggf. technisch und/oder organisatorisch ersetzbar wäre. Der Ansatz unterscheidet dementsprechend die Exposition von Komponenten und Prozessen, die Funktionsanfälligkeit und die verschiedenen Formen der Ersetzbarkeit. (Krings, in Druck, S. 25 f)

Für die Durchführung der Analyse nach Krings (in Druck) sind Daten der öffentlichen und privaten Akteure, die sich den Betrieb und Besitz Kritischer Infrastruktur auf kommunaler Ebene teilen, erforderlich. Diese Daten befinden sich sowohl in der Hand der Infrastrukturbetreiber – es besteht aus diversen Gründen das Interesse die Daten vertraulich zu behandeln – als auch bei den jeweiligen Kommunen. Folglich können die exponierten Komponenten nur gemeinsam mit den Betreibern (auf kommunaler Ebene) analysiert und ihre Bedeutung für den gesamten Prozess der Stromversorgung eingeordnet werden, um ein Gesamtbild der Situation entstehen zu lassen. Aufgrund der großen Menge an Detailinformationen der Einzelaspekte von Funktionsanfälligkeit oder Bewältigungskapazität sowie der vertraulich behandelten Daten auf Betreiberseite



können nur bedingt allgemeingültige Aussagen zu den Einflussfaktoren von Funktionsanfälligkeit oder Bewältigungskapazität getroffen werden. Vielmehr ermöglicht das Konzept eine Analyse der konkreten Versorgungslage vor Ort unter Annahme bestimmter Szenarien. Auch werden Möglichkeiten der Bewältigungskapazität, wie beispielsweise Redundanzen, erst in einem späteren Schritt berücksichtigt (siehe Krings, in Druck).

Zwar ist der Ansatz des Konzepts, Verwundbarkeit als Funktion aus Exposition, Anfälligkeit und Bewältigungskapazität zu betrachten, an das grundsätzliche Verständnis von Vulnerabilität angelehnt. Das Konzept ist jedoch insbesondere im Zusammenhang mit konkreten Ereignissen oder Szenarien auf kommunaler Ebene anwendbar. Eine allgemeine Verwundbarkeitsbemessung für Deutschland ist jedoch nicht möglich, weshalb das Konzept im Rahmen dieser Studie nicht verwendet werden kann.

### 3.3.3 Verwundbarkeitsabschätzung nach Baker

In Anlehnung an Dokumente des Department of Homeland Security der USA bezüglich Kritischer Infrastrukturen und deren Verwundbarkeitsbemessung entwickelte Baker (2005) eine allgemeine Methode zum Vulnerabilitätsassessment. Ähnlich wie in den beiden zuvor dargelegten Konzepten werden auch in dem Ansatz von Baker in einem ersten Schritt der Verwundbarkeitsabschätzung die Gefahren, denen Infrastrukturen ausgesetzt sind, bestimmt. Dabei geht Baker insbesondere auf Naturgefahren und kriminelle Handlungen ein. Neben der Wahrscheinlichkeit und der Schwere des Ereignisses, werden zudem auch Erfahrungen aus vergangenen Schadensereignissen in die Analyse mitaufgenommen. Fragen wie:

- Welche vergangenen Ausfälle gab es und was war die Ursache?
- Welche Infrastruktursysteme waren betroffen?
- Welche Kaskadeneffekte waren zu beobachten?

sowie dazugehörige Daten sind dabei von Relevanz. Zudem sind Aufgabe und Funktion der jeweiligen Kritischen Infrastruktur sowie deren Verknüpfungen und Abhängigkeiten von anderen Kritischen Infrastrukturen als Grundlage für die Analyse von besonderer Bedeutung. Redundanzen, Substituierbarkeit, Back-up-Systeme oder Wiederherstellungsgeschwindigkeit des alten Zustands sind weitere Eigenschaften des Systems die in die Bewertung miteinbezogen werden. Abgesehen von den technischen Reaktionsmöglichkeiten, werden auch die Fähigkeit und Kompetenz der Mitarbeiter in Krisen- und Notfallsituationen richtig zu reagieren, in der Analyse berücksichtigt. Untersucht wird, ob Mitarbeiter ausreichend für derartige Ereignisse ausgebildet und/oder Notfall- und Evakuierungspläne vorhanden sind (Baker, 2005, S. 4 ff).



Im Vergleich zu den oben erwähnten Konzepten nimmt der Ansatz zwar keine wörtliche Unterteilung der Analyse in Exposition, Anfälligkeit und Bewältigungskapazität vor, betrachtet aber systematisch die Indikatoren Exposition (gegenüber Gefahren), Anfälligkeit (Abhängigkeit von anderen Infrastrukturen, Fähigkeiten und Kompetenz der Mitarbeiter, technische Reaktionsmöglichkeiten, usw.) und Bewältigungskapazität (Redundanzen, Substituierbarkeit, Back-up-Systeme, usw.). Zudem werden die genannten Komponenten des Systems unterschiedlich gewichtet und im Anschluss gemeinsam ausgewertet – unklar bleibt jedoch die Art der Gewichtung und Auswertung. Das Ergebnis ist eine Verwundbarkeitsabschätzung je nach Gefahrentyp, in Form einer Matrix (siehe Abbildung 8), die unterschiedliche KRITIS mit verschiedenen Gefahren zusammenführt. Eine schriftliche Zusammenfassung der Ergebnisse empfiehlt sich zudem als Grundlage für die Entwicklung von Strategien zur Verbesserung der Belastbarkeit des Systems gegenüber Gefahren (Baker, 2005, S. 9).

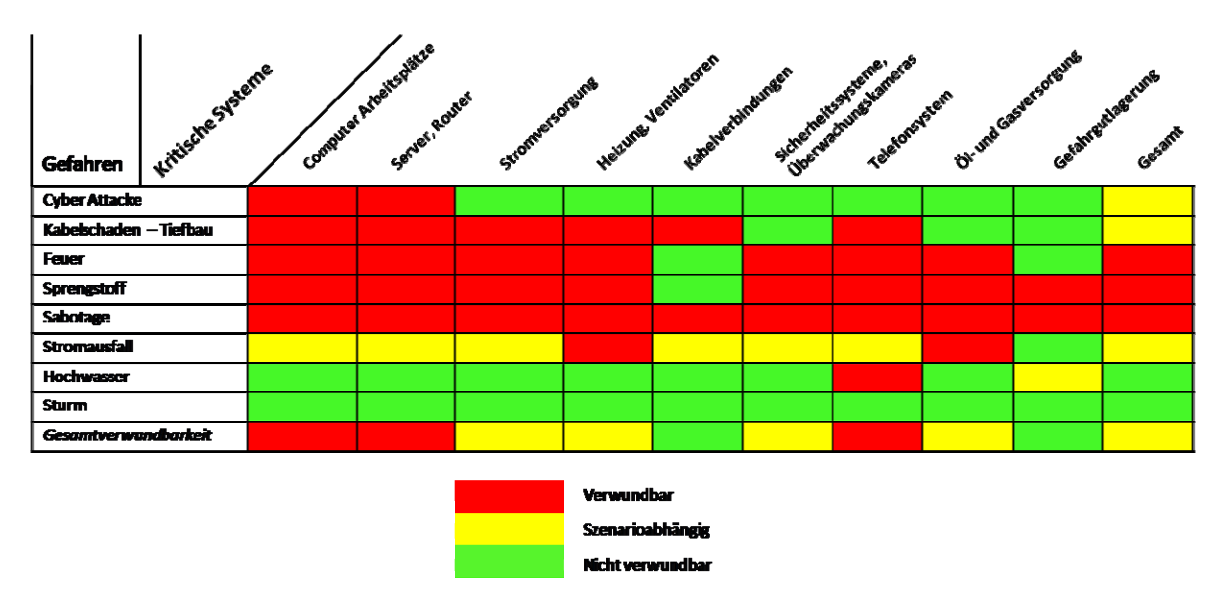



**Abbildung 8: Verwundbarkeitsabschätzung nach Baker**

Quelle: (eigene Darstellung in Anlehnung an (Baker, 2005, S. 10))

Das Konzept nach Baker (2005) ermöglicht zwar eine allgemeine Anwendung und Übertragbarkeit auf die regionale/nationale Ebene – im Vergleich zum Modell von Krings –, die Gewichtung der einzelnen Komponenten, sowie das Gesamtergebnis sind jedoch nicht nachvollziehbar. Zudem ist nicht erkennbar welche Bewertungsgrundlage für die Unterteilung in *verwundbar*, *szenarioabhängig* und *nicht verwundbar* gewählt wurde, weshalb auch dieses Konzept im weiteren Verlauf keine Verwendung findet.

Abschließend lässt sich festhalten, dass die vorgestellten Konzepte das Verständnis der Verwundbarkeit als Funktion von Exposition, Anfälligkeit und Bewältigungskapazität



zugrunde legen. Diese Gemeinsamkeit der Ansätze zur Verwundbarkeitsabschätzung von KRITIS soll deshalb auch im Rahmen dieser Studie aufgegriffen werden. Tabelle 2 zeigt beispielhaft die Komponenten der Vulnerabilität der Kritischen Elektrizitätsinfrastruktur.

**Tabelle 2: Komponenten der Verwundbarkeit Kritischer Infrastrukturen und ausgewählte Beispiele**

| **Exposition** | **Anfälligkeit** | **Bewältigungskapazität** |
|---|---|---|
| Naturgefahren<br><br>(z.B. Hochwasser oder Sturm) | Fortschreitende Privatisierung | Dezentralisierung |
| Kriminelle Handlungen<br><br>(z.B. Cyberattacke oder Terroranschlag) | Komplexität des Systems | Back-up Systeme |
| | Technisches/menschliches Versagen | Notstromaggregate |

Quelle: (eigene Darstellung)



# 4 Verwundbarkeit der Elektrizitätsversorgung

Wie eingangs beschrieben, bestehen zwar verschiedenste Konzepte zur Abschätzung der Verwundbarkeit von Kritischen Infrastrukturen (siehe Kapitel 3), jedoch ähneln sich diese in der Zusammensetzung ihrer Komponenten, die sich in die drei Bereiche *Exposition*, *Anfälligkeit* und *Bewältigungskapazität* gliedern lassen. Entsprechend wird die Vulnerabilität der Elektrizitätsinfrastruktur im Folgenden anhand dieser Bereiche analysiert.

## 4.1 Exposition

| f (Vulnerabilität) = **Exposition (Gefahr)**, Anfälligkeit, Bewältigungskapazität |
|---|

Um die Vulnerabilität verschiedener Komponenten, und damit auch der jeweiligen Prozesse, einschätzen zu können, bedarf es zunächst einer Analyse der Komponenten gegenüber unterschiedlichen Gefahren, wobei im Folgenden in Anlehnung an das BMI zwischen Naturgefahren und von Menschen verursachten Gefahren (Terroranschlägen und Cyberattacken) unterschieden wird.

> *„Die staatliche und gesellschaftliche Aufmerksamkeit muss deshalb vor allem zwei Gefährdungsursachen gelten: einmal der terroristischen Bedrohung und darüber hinaus den in ihrer Bedeutung für die Infrastrukturen wachsenden Naturgefahren.“* (BMI, 2009, S. 8)

### 4.1.1 Naturgefahren

Um die Exposition von Kritischen Infrastrukturen gegenüber Naturgefahren abschätzen zu können, muss in einem ersten Schritt identifiziert werden, welche Naturgefahren den Lebens- und Wirtschaftsraum Deutschland bedrohen. Dazu ist in Tabelle 3 eine Übersicht über mögliche Naturgefahren in Deutschland dargestellt. Wie man ihr entnehmen kann, haben die Naturgefahren unterschiedlich starke räumliche sowie zeitliche Ausprägungen (Merz & Emmermann, 2006, S. 266 ff).

Dabei wird schnell ersichtlich, dass nur wenige Naturgefahren räumlich zu verorten sind. So können beispielsweise Hagel, Wald- und Heidebrände sowie seismische und kosmische Ereignisse über ganz Deutschland hinweg beobachtet werden, während Sturmfluten in den Küstengebieten oder Hochwasser im Bereich von Flussläufen auftreten[6]. Daraus folgt, dass Kritische Infrastrukturen, welche sich an Flüssen und

[6] Das BMI fasst zudem Epidemien und Pandemien bei Mensch, Tier und Pflanzen als Naturereignis auf, das KRITIS bedrohen kann (BMI, 2009, S. 7). Diese werden jedoch im Rahmen dieser Studie vernachlässigt.



dabei speziell in Gebieten, die als potentielle Überflutungsbereiche dienen, besonders gefährdet sind. Beispielhaft für die Exposition Kritischer Infrastrukturen gegenüber Hochwassern und deren sozialen und ökonomischen Folgen, kann das Elbehochwasser im August 2002 herangezogen werden. Das Hochwasser zerstörte zahlreiche Straßen, Bahnlinien, Haupt-Transformatoren und Umspannstationen und führte somit zu einem enormen Ausfall an Infrastruktureinrichtungen in nahezu allen Bereichen. Durch die wichtige Erkenntnis, dass Extremereignisse solchen Ausmaßes auch in Deutschland eintreten können, ist die Risikoabschätzung für diese seltenen Ereignisse für sämtliche Infrastruktur-Sektoren empfehlenswert (Lauwe & Riegel, 2008, S. 116).

Neben der räumlichen Ausbreitung der Naturgefahren sind auch hinsichtlich der Dauer der Ereignisse große Unterschiede vorhanden. Während ein Hagelereignis tendenziell einige Minuten bis Stunden andauert, kann eine Hitzewelle einige Tage bis Wochen anhalten (Merz & Emmermann, 2006, S. 266 ff). Schließlich ist darin ein Unterschied zu sehen, dass die Vorhersage sowie die möglichen Vorbereitungen auf ein Naturereignis stark variieren. Während es beispielsweise bei einem Hochwasserereignis zum Teil möglich ist, eine Vorhersage sowie Vorbereitungen zu treffen, ist dies bei einer Hitzewelle wesentlich schwieriger. Beispielsweise gilt es im Umgang mit einem Hochwasser auf der Grundlage von Szenarien frühzeitig Pläne auszuarbeiten, in denen die möglicherweise exponierten Gebiete und die damit betroffenen Objekte identifiziert werden (siehe hierzu auch Birkmann et al., in Druck).

**Tabelle 3: Übersicht über mögliche Naturgefahren und ihre räumliche sowie zeitliche Komponente**

| **Naturgefahr** | **Gefährdete Gebiete in Deutschland** | **Raumskala** | **Dauer von Ereignissen**[7] |
|---|---|---|---|
| *Hagel* | Deutschlandweit, landeinwärts zunehmend, besonders Voralpen | Einige 10 km bis wenige 100 km | Einzelereignis: < eine Stunde; Gesamtereignis: einige Stunden |
| *Blitzschlag* | Deutschlandweit | Einige 10 km; Gruppen von Gewitterzellen: mehrere 100 km | Einzelereignis: < eine Stunde; Gesamtereignis: einige Stunden |
| *Tornado* | Deutschlandweit, vor allem Ebenen, besonders Nordwestdeutschland | Durchmesser: einige m bis 500 m; Zuglänge: wenige 10 km bis 100 km | Wenige Sekunden bis > eine Stunde, durchschnittlich < zehn Minuten |

[7] „Unter Gesamtereignis werden alle Einzelereignisse bezeichnet, die durch dasselbe Ereignis ausgelöst werden. So gelten die Hochwasser vom August 2002 als ein Gesamtereignis, da durch dieselbe Großwetterlage verursacht. Innerhalb dieser Gesamtereignisse lassen sich mehrere Einzelereignisse unterscheiden, etwa die Flusshochwasser Elbe und Donau sowie Sturzfluten im Erzgebirge.“ ((Merz & Emmermann, 2006, S. 268) zitiert nach (DKKV), 2003).



| *Wintersturm* | Deutschlandweit, besonders im Westen | Windfeldbreite bis über 1.000 km, Zuglänge bis zu 5.000 km | Wenige Stunden bis wenige Tage |
|---|---|---|---|
| *Starkniederschlag, Sturzflut* | Deutschlandweit | Lokal, < einige 10 km; Gruppen von Niederschlagsfeldern: mehrere 100 km | Wenige Stunden |
| *Flusshochwasser* | Deutschlandweit in Flusstälern | Mehrere 10 km bis mehrere 100 km | Wenige Stunden bis einige Tage |
| *Sturmflut* | Nordseeküste, schwächer auch Ostseeküste | Einige 100 km | Wenige Stunden bis wenige Tage |
| *Trockenheit, Dürre* | Deutschlandweit | Mehrere 100 km bis mehrere 1.000 km | Einige Wochen bis wenige Monate |
| *Kältewelle, Hitzewelle* | Deutschlandweit | Bis mehrere 1.000 km | Einige Tage bis wenige Monate |
| *Waldbrand* | Deutschlandweit, besonders im Nordosten | Einzelereignis: einige 10 km, Gesamtereignis: über mehrere 100 km | Einige Stunden bis mehrere Tage |
| *Schneesturm* | Deutschlandweit | Bis einige 100 km | Einige Stunden bis wenige Tage |
| *Lawine* | Alpen | < 1 km | Minuten |
| *Rutschung, Berg-/Felssturz, Mure* | Alpen und Mittelgebirge | < 1 km | Sekunden bis Minuten |
| *Erdbeben* | Erdbebengefährdete Gebiete | < 100 km | Wenige Minuten; Nachbeben: einige Tage |
| *Vulkanausbruch* | Eifel | Atmosphärischer Transport: mehrere 100 km; stratosphärischer Transport: mehrere 1.000 km | Einige Stunden bis mehrere Tage; indirekte Folgen: Monate |
| *Magnetischer Sturm* | Deutschlandweit, stärkere Gefährdung in Norddeutschland | Mehrere 100 km | Ein Tag, in Einzelfällen mehrere Tage |
| *Meteoriteneinschlag* | Deutschlandweit | Krater: bis 300 km; globale Auswirkungen möglich, etwa auf das Klima | Minuten; bei großen Einschlägen langandauernde Folgen |

Quelle: (Merz & Emmermann, 2006, S. 268)

Des Weiteren müssen auch in Deutschland die Auswirkungen des globalen Klimawandels beachtet werden. Auf globaler Ebene beschreibt der Intergovernmental Panel on Climate Change (IPCC) dabei, dass *„auf der Skala von Kontinenten, Regionen und Ozeanbecken [...] zahlreiche langfristige Änderungen des Klimas beobachtet [wurden].*



*Zu diesen gehören Änderungen der Temperaturen und des Eises in der Arktis sowie verbreitet Änderungen in den Niederschlagsmengen, im Salzgehalt der Ozeane, in Windmustern und bei Aspekten von extremen Wetterereignissen wie Trockenheit, Starkregenniederschlägen, Hitzewellen und der Intensität von tropischen Wirbelstürmen*" (IPCC, 2007b, S. 7). Auch für die Zukunft wird prognostiziert, dass bei andauernd gleich hohen oder gar höheren Treibhausgasemissionen der Anstieg der globalen Mitteltemperatur weiter beschleunigt wird. Es wird zudem in höheren Breiten sehr wahrscheinlich mit einer Zunahme der Niederschläge gerechnet. Schließlich wird angenommen, dass Extremereignisse wie Hitzewellen und Starkniederschlagsereignisse höchstwahrscheinlich weiter zunehmen werden[8] (IPCC, 2007b, S. 7; Zebisch et al., 2005, S. 5f).

Die tendenzielle Zunahme sogenannter Extremereignisse (Wetterextreme) kann auch für die Sicherheit der KRITIS Elektrizitätsversorgung ein erhebliches Problem darstellen. Beispiele für vergangene Extremereignisse in Deutschland können in der, Hitzewelle 2003, den Hochwassern an Rhein 1993 und 1995, Elbe 2002 und Oder 2005 sowie in den Stürmen Lothar 1999 und Kyrill 2007 gesehen werden (Birkmann & Krings, 2008, S. 25; Reichenbach et al., 2008, S. 37 f; Geier et al., 2005, S. 9 ff). Mögliche Wirkfolgen entsprechender Naturgefahren werden daher im Folgenden eingehender analysiert. Zuvor soll allerdings eine naturräumliche Gliederung Deutschlands durchgeführt werden, um – unter Berücksichtigung von Szenarien bezüglich des Klimawandels – aufzuzeigen, welche deutschen Regionen mit den in ihr vorhandenen KRITIS gegenüber welchen Naturgefahren besonders exponiert sind (siehe Abbildung 9).

In *Ostdeutschland (Norddeutsches Tiefland und Südostdeutsche Becken und Hügel)* besteht beispielsweise eine hohe Exposition gegenüber Dürren, die durch eine geringe Wasserverfügbarkeit und hohe Temperaturen in den Sommermonaten bedingt ist. Dieser Zustand kann sich weiter zuspitzen, wenn die Sommerniederschläge zukünftig weiter zurückgehen und durch die steigenden Temperaturen eine höhere Verdunstung in Oberflächengewässern erfolgt. In den Einzugsgebieten von Oder und Elbe kommt hinzu, dass diese Gebiete einem hohen Hochwasserrisiko ausgesetzt sind (Zebisch et al., 2005, S. 166; Die Bundesregierung, 2008, S. 49).

In *Südwestdeutschland (Oberrheingraben)* wird mit dem stärksten Temperaturanstieg gerechnet, wobei die Temperaturen schon heute die Höchstwerte Deutschlands erreichen. In Südwestdeutschland ist demzufolge die Exposition gegenüber Hitzewellen besonders ausgeprägt. Außerdem ist diese Region durch Hochwasser im frühen Frühjahr gefährdet. Diese können zum einen durch eine Verschiebung der Nieder-

[8] Dies ist nur eine Auswahl an Projektionen zukünftiger Änderungen des Klimas. Für weitere Projektionen siehe IPPC (2007)b.



schläge von den Sommer- in die Wintermonate ausgelöst werden, zum anderen kann die mögliche Zunahme von Starkregenereignissen zu Hochwassern führen (Zebisch et al., 2005, S. 166; Die Bundesregierung, 2008, S. 49; Reichenbach et al., 2008, S. 38).

Die deutschen *Mittelgebirge* zeichnen sich durch ein eher kühles, feuchtes Klima aus, sodass eine mögliche Klimaerwärmung eher ausgeglichen werden kann als das in anderen Regionen Deutschlands der Fall ist. Dennoch ist auch die Region Mittelgebirge gegenüber Hochwassern exponiert, die durch konvektive Starkniederschläge verursacht werden können (Zebisch et al., 2005, S. 167).

Im *Küstengebiet* wird im Zusammenhang mit dem Klimawandel mit einem vergleichsweise geringen Lufttemperaturanstieg[9] gerechnet, dennoch wird sich voraussichtlich die Häufigkeit von Temperaturkenntagen verändern, welche sich in Eis-, Frost- und Sommertagen oder Tropennächten äußern. Zudem wird angenommen, dass trockenere Sommer und niederschlagsreichere Winter eine Folge sein werden. Schließlich liegt eine Exposition durch tendenziell steigende Meeresspiegel und eventuell intensivere Sturmfluten als mögliche Folgen des Klimawandels vor (Zebisch et al., 2005, S. 167; Die Bundesregierung, 2008, S. 48; Reichenbach et al., 2008, S. 37).

[9] Als Grund dafür wird die Nähe zum Meer sowie das relativ ausgeglichene und gemäßigte Küstenklima angegeben (Reichenbach et al., 2008, S. 37; Die Bundesregierung, 2008, S. 48).



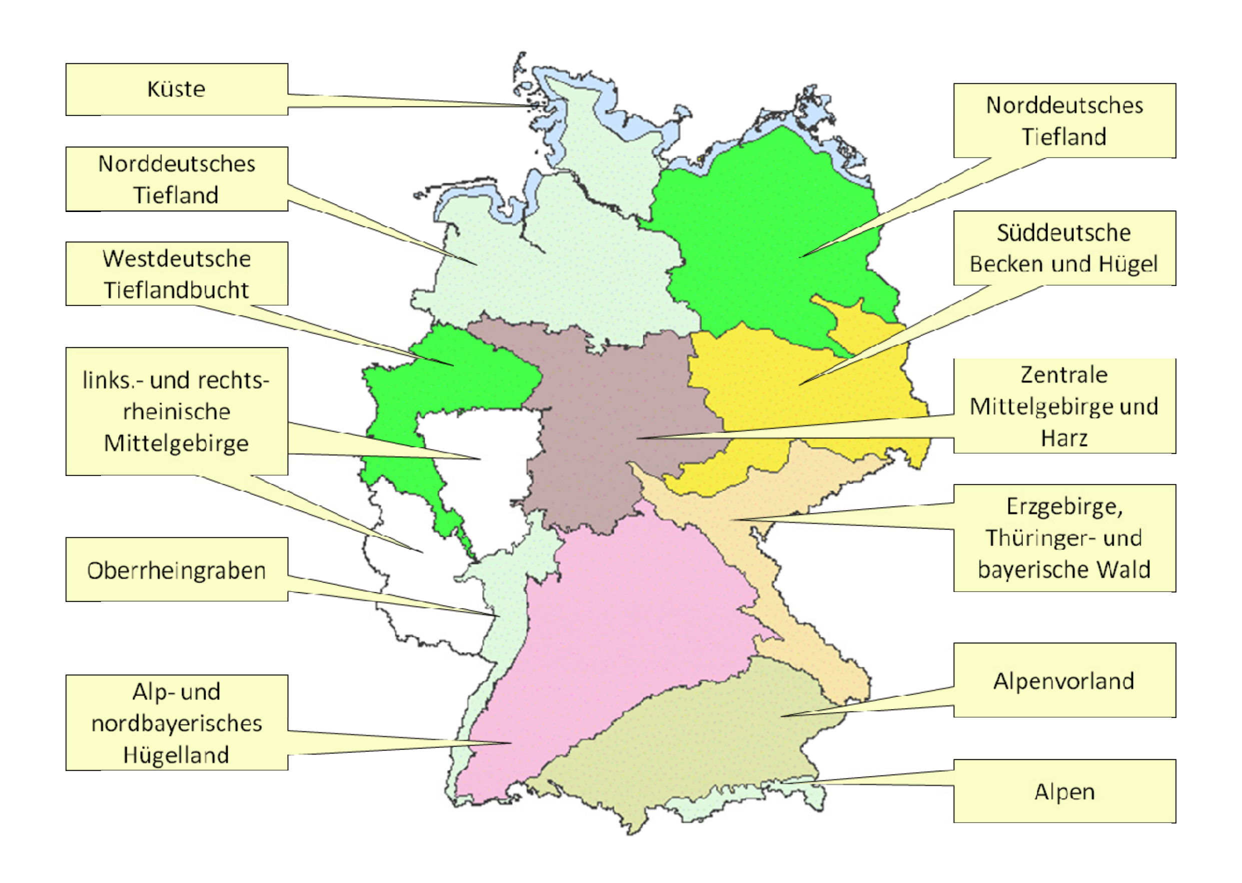



**Abbildung 9: Naturräumliche Gliederung Deutschlands**

Quelle: (Zebisch et al., 2005, S. 166)

Hinsichtlich der Exposition sind auch Unterschiede darin zu sehen, welche Auswirkungen eine Naturgefahr auf die Stromversorgung hat. Bei einem Hochwasserereignis gelten Stromausfälle oftmals als Begleiterscheinungen, da durch die Überflutung die lokale Mittel- und Niedrigspannung betroffen sein kann. Kommt es zu einem Ausfall des Stromnetzes, so ist dieser meistens auf das Überschwemmungsgebiet und einige angrenzende Bereiche beschränkt. Dies hängt damit zusammen, dass oftmals nur diejenigen Komponenten und Anschlüsse vom Netz genommen werden, die auch akut vom Hochwasser betroffen sind. Ist eine Kommune – innerhalb des Überschwemmungsgebietes – auf ein Hochwasser vorbereitet, so ist die Stromversorgung meistens auch für Kommunen außerhalb des Überschwemmungsgebiets gesichert. Ist allerdings die Vorbereitung vom Hochwasser betroffener Kommunen ungenügend oder nicht vorhanden, so kann es auch weiter entfernt von der eigentlichen Überschwemmung zu Stromausfällen beziehungsweise Leistungseinschränkungen der Stromversorgung kommen (Birkmann & Krings, 2008, S. 26 f).



Im Gegensatz zum Hochwasser, wo die Störung der Stromversorgung unmittelbar mit dem Überschwemmungsgebiet in Zusammenhang steht, kann es beispielsweise bei Hitzewellen zu überregionalen Auswirkungen kommen. Zudem kommt es oftmals zu einem erhöhten Stromverbrauch der Bevölkerung, der im deutlichen Gegensatz zu der tendenziell reduzierten Stromproduktion in der Hitzewelle steht. Dieser resultiert vor allem aus der vermehrten Nutzung von Klimaanlagen und Kühlsystemen in Privathaushalten und der Wirtschaft. Diesem Phänomen steht eine geringere Kraftwerksleistung gegenüber, da die Kühlwassereinleitung in die Flüsse nur noch eingeschränkt möglich ist, um den Grenzwert der Gewässertemperatur von 28°C[10] nicht zu überschreiten. Somit müssen während extremer Hitzeperioden – wie beispielsweise der Hitzewelle 2003 – Kraftwerke in ihrer Leistung gedrosselt oder abgeschaltet werden (Lange, 2009, S. 5 ff). Ferner ist die räumliche Ausdehnung der Hitzewelle wesentlich größer (Merz & Emmermann, 2006). Zusammenfassend kann nun festgehalten werden, dass bei einem Hochwasserereignis eher punktuell im Bereich der Überschwemmung Beeinträchtigungen des Stromnetzes vorhanden sind und dabei das Naturereignis selbst den Stromausfall auslöst. Im Gegensatz dazu ist bei einer Hitzewelle nicht die Zerstörung von einzelnen Komponenten dafür verantwortlich, dass es zu Sicherheitsproblemen bei der Versorgung mit Strom kommt. Vielmehr sind es hier veränderte Umweltbedingungen, von denen Kraftwerke und damit die Stromversorgung abhängig ist (Birkmann & Krings, 2008, S. 28 f; Kropp et al., 2009, S. 180 ff; Lange, 2009, S. 5 ff).

Ein weiterer Punkt, der bei der Untersuchung der Exposition Kritischer Infrastrukturen gegenüber Naturgefahren beachtet werden muss, ist die Tatsache, dass generell oberirdische Komponenten der Kritischen Infrastrukturen stärker exponiert sind als unterirdisch verlegte Komponenten (Brakelmann, 2006, S. 2). Betrachtet man wieder das Beispiel eines Hochwasserereignisses, so sind die unterirdisch verlegten Leitungen bei einem solchen Ereignis nicht direkt exponiert. Allerdings können diese durch Erosion freigelegt und damit exponiert werden. Speziell Leitungen, welche an Brücken angebracht, in Böschungen verlegt sind oder an Knotenpunkten an die Oberfläche kommen, sind besonders gegenüber der Hochwassergefahr exponiert (Krings, in Druck, S. 30). Oberirdische Leitungen sind besonders bei Stürmen oder starken Schneefällen exponiert, wie der Stromausfall im Münsterland 2005 verdeutlichte (siehe Kapitel 4.1.3). Denn Strommasten sowie Oberleitungen können durch die Einwirkung bestimmter Naturgefahren umknicken, zusammenbrechen oder reißen (siehe Abbildung 10).

[10] Theoretisch ist es möglich Kraftwerke auch mit höherer Wassertemperatur zu kühlen, allerdings erhöht sich dadurch auch die Wassertemperatur des zurückzuführenden Wassers. Grund für diese Grenzwerte der Wasserrückführung ist vor allem der Schutz der Gewässerökologie. Denn diese wird bei einer zu starken Erwärmung der Flüsse gestört (Lange, 2009, S. 5 ff).





**Abbildung 10: Strommasten knicken um wie Streichhölzer.**

Quelle: (focus-online, 2006).

Je nachdem, welche Komponenten und Prozesse betroffen sind (siehe dazu auch Kapitel 2), hat dies auch Auswirkungen darauf, wie groß die Störung des Stromnetzes insgesamt ist. So kann beispielsweise bei der Zerstörung einer Hochspannungsleitung, die Stromversorgung größerer Regionen beeinträchtigt werden (siehe hierzu auch Kapitel 4.1.3 Beispiel Stromausfall Münsterland). Somit ist es von großer Bedeutung, welche Stellung die Komponente oder der Prozess der von der Kritischen Infrastruktur betroffen ist für die Funktionsfähigkeit des Gesamtsystems hat. Je nach Reichweite der Stromnetze, die an die Komponente oder den Prozess gekoppelt sind, können somit unterschiedlich viele Menschen von der Beeinträchtigung der Stromversorgung betroffen sein (Krings, in Druck, S. 40 ff). So sind beispielsweise bei dem Stromausfall im Münsterland im November 2005 mehrere Komponenten zerstört worden, da durch hohe Schneelast, Starkwind und Eisregen Stromleitungen gerissen sowie Strommasten umgeknickt sind. Durch die Zerstörung dieser Komponenten wurde der Prozess des Stromtransports gestört, sodass etwa 250.000 Menschen von der Stromversorgung abgeschnitten waren (siehe dazu ausführlicher Kapitel 4.1.3) (CONSENTEC et al., 2008, S. 136 f). Im Gegensatz dazu gibt es auch Stromausfälle, die nicht durch die Beschädigung von Komponenten ausgelöst werden, sondern durch einen Eingriff oder durch die Überlastung von Prozessen entstehen. So wurde im November 2006 eine geplante Abschaltung einer 380-kV-Leitung durchgeführt um einen Schiffstransport von der Ems in die Nordsee zu ermöglichen. Dabei wurden allerdings Sicherheitskriterien nicht eingehalten, sodass es zu kaskadenartigen Abschaltungen von



Übertragungsleitungen kam, und. etwa 10 Millionen Menschen in vielen Ländern Europas von dem Stromausfall betroffen waren (siehe dazu ausführlicher Kapitel 4.1.3) (CONSENTEC et al., 2008, S. 136 ff).

### 4.1.2 Kriminelle Handlungen

Neben den bereits erläuterten Naturgefahren, können Kritische Infrastrukturen auch *Terrorismus, Sabotage, sonstige Kriminalität* und *Krieg* ausgesetzt sein (BMI, 2009, S. 7). Im Folgenden werden mögliche Auswirkungen dieser Gefährdungen untersucht, sind jedoch eher als Exkurs zu verstehen.

Reichenbach et al. (2008) sehen im Grünbuch des Zukunftsforums Öffentliche Sicherheit eine Bedrohung für Deutschland besonders durch *Terrorismus* und *Organisierte Kriminalität* insbesondere mittels des Internets, weshalb im Folgenden auf diese beiden Gruppen näher eingegangen wird. Terrorismus wird als politisch oder ideologisch motiviert bewertet, wobei die öffentliche Aufmerksamkeit und das Verbreiten von Angst im Vordergrund stehen (Reichenbach et al., 2008, S. 28 f). Ausgeübte oder angedrohte Gewalttaten gegenüber Menschen, Objekten oder Infrastrukturen sollen Schrecken in der Bevölkerung verbreiten, um dadurch Einfluss auf staatliche Organe zu nehmen (Benzin, 2005, S. 38). „*Organisierte Kriminalität ist die von Gewinn- und Machstreben betsimmte planmäßige Begehung von Straftaten, die einzeln oder in ihrer Gesamtheit von erheblicher Bedeutung sind*“ (Reichenbach et al., 2008, S. 28 f).

Aufgrund der immer stärkeren Interdependenz einzelner Infrastruktursysteme und der damit einhergehenden Möglichkeit durch die Störung einer Infrastruktur erhebliche Kettenreaktionen und Schäden auszulösen, sind kriminelle Handlungen gegenüber Kritischen Infrastrukturen in den Fokus staatlicher Schutz- und Sicherheitsanstrengungen gerückt. Besonders seit dem 11. September 2001 hat die Bedrohung durch den internationalen Terrorismus als Gefahrenszenario für KRITIS an Bedeutung zugenommen. Dabei wurden insbesondere die engen Verflechtungen und die damit einhergehende Verwundbarkeit moderner Gesellschaften aufgrund der Abhängigkeit von KRITIS deutlich (BMI, 2009, S. 7; Hanning, 2008, S. 40). Aus diesem Grund wird im folgenden Kapitel explizit auf terroristische Gefahren gegenüber Kritischen Infrastrukturen eingegangen. Da jedoch die Informationstechnik den zusammenlaufenden Knotenpunkt des Schutzes Kritischer Infrastrukturen bildet und elementare, für das Gemeinwesen erforderliche, Versorgungseinrichtungen innerhalb moderner Industriegesellschaften vernetzt (Greve, 2009, S. 758), wird im zweiten Abschnitt (Kapitel 0) das Gefahrenpotenzial durch Cyberattacken näher erläutert.



## Exposition gegenüber Terrorismus

Speziell nach den terroristischen Anschlägen in den USA 2001 und Europa (London 2005 und Madrid 2004) (merkur-online, 2007), wurden staatliche Sicherheitsanstrengungen bezüglich exponierter Kritischer Infrastrukturen verschärft. Auch Infrastrukturen in Deutschland sind zunehmend Zielobjekte des internationalen Terrorismus (Beispiel Sauerland-Gruppe) (Hufelschulte, 2006); durch gezielte Anschläge auf Schlüsselelemente Kritischer Infrastrukturen können dabei lang anhaltende und weiträumige Schäden verursachen werden.

In Deutschland wurde daher im Jahr 1997 u.a. die Arbeitsgemeinschaft Kritische Infrastrukturen (AG KRITIS) zum Aufbau einer Organisation und Struktur zum Schutz Kritischer Infrastrukturen ins Leben gerufen. Diese soll Schwachstellen der Systeme ermitteln und Möglichkeiten zur Behebung oder Minderung der Schäden erarbeiten (Kuhn & Neuneck, 2005, S. 14; Lauwe & Riegel, 2008, S. 115; Kuhn, 2005, S. 3).

Generell stellen alle Energieträger, sowie deren Infrastruktur Angriffsziele für terroristische Handlungen dar, sodass Komponenten der herkömmlichen und erneuerbaren Energien betroffen sein können (siehe hierzu auch Abbildung 3 Kapitel 2). Bisher kam es jedoch in Deutschland weder zu einem größeren Zwischenfall bei Öl- und Gaspipelines noch zu Anschlägen auf Weiterverarbeitungsindustrien oder Kraftwerke. In politisch fragileren Regionen, wie z.B. in der Türkei (sueddeutsche.de, 2010) oder im Kaukasus (Bender, 2010) zeigen Anschläge auf solche Infrastrukturen jedoch, dass Pipelines ein beliebtes Ziel krimineller Handlungen sein können, da sie erheblichen ökonomischen Schaden mit sich bringen. Auch Höchst- und Hochspannungsleitungen sowie Transformatoren-Stationen sind gegenüber terroristischen Anschlägen sehr verwundbar. Besonders der Austausch zerstörter Transformatoren würde länger dauern, da derartige Geräte oftmals nicht in ausreichender Zahl vorrätig sind und der Transport dieser Anlagen einige Zeit in Anspruch nimmt (Shull, 2006, S. 9). Eine Unterbrechung der Stromversorgung kann aufgrund des Zusammenwirkens unterschiedlicher Infrastrukturbereiche enorme Schäden und Versorgungsausfälle verursachen (EU-Kommission, 2004, S. 3). Auf sogenannte Kaskadeneffekte und das komplexe Zusammenwirken unterschiedlicher Kritischer Infrastrukturen wird in Kapitel 5.3 näher eingegangen.

Ein im Zusammenhang mit Terroranschlägen häufig genanntes Zielobjekt in Deutschland sind Kernkraftwerke (KKW), deren Zerstörung durch terroristische Aktivitäten verheerende Auswirkungen für die Gesellschaft haben würde. Bisher sind die meisten KKWs in Deutschland soweit ausgestattet, dass mögliche Angriffe durch Kampfjets abgewehrt, Unfälle mit Passagierflugzeugen jedoch gefährlich werden können (Kuhn & Neuneck, 2005, S. 8; Lauwe & Riegel, 2008, S. 118).



Die in Abbildung 11 dargestellte Deutschlandkarte liefert einen Überblick über die aktuellen Standorte deutscher Kernkraftwerke sowie die damit einhergehende räumliche Verteilung möglicher terroristischer Zielobjekte. Dabei fällt besonders die Konzentration der Anlagen im Südosten sowie im Norden Deutschlands auf. Die Kürzel unter den jeweiligen Kernkraftwerken sind deren Bezeichnung, die nebenstehende Zahl ist die Bruttoleistung in MW. Des Weiteren ist allerdings bisher wenig über die Anfälligkeit und Bewältigungskapazitäten solcher potenziellen Ereignisse bekannt.




**Abbildung 11: Risikokarte Deutschland: Kernkraftwerke**

Quelle: (BfS, o.J.)

Störfälle in deutschen Kernkraftwerken müssen seit 1975 nach bundeseinheitlichen Meldekriterien an das Bundesamt für Strahlenschutz (BfS) gemeldet werden (BfS, 2010). Mit der Einführung der „International Nuclear Event Scale“ (INES) im Jahr 1989 – die Skala beinhaltet neben den Ereignissen in Kernkraftwerken auch kerntechnische Anlagen, den Transport, die Lagerung und die Nutzung von radioaktiven Stoffen –



werden gemeldete Störfälle je nach Schwere kategorisiert. Anschläge auf Kritische Infrastrukturen in Deutschland sind seitdem nicht registriert worden. Von den über 2.300 meldepflichtigen Ereignissen deutscher Kernkraftwerke zwischen 1994 und 2004 wurde keines der Zwischenfälle höher als Stufe 2 (Störfall) eingestuft (siehe Abbildung 12) (Borst et al., 2006; IAEA, 2010). Ein solcher Störfall führt laut Bundesamt für Strahlenschutz (BfS) zu einer erheblichen Strahlenkontamination innerhalb der Anlage, weshalb in diesem Fall besonders das Personal der Anlagen einer unzulässig hohen Strahlenexposition ausgesetzt ist. Erst bei der nächsthöheren Stufe in der Skala wäre auch die Bevölkerung außerhalb der Anlagen erheblich betroffen (BfS, 2010). Ein terroristischer Angriff auf KKWs hat zwar aufgrund der enormen Strahlenbelastung verheerende Auswirkungen für die Bevölkerung, jedoch ist, auch aufgrund des relativ geringen Beitrags der Kernenergie von 23% zur Bruttostromerzeugung in Deutschland (siehe auch Kapitel 2) fraglich, welche Bedeutung der Ausfall eines Kernkraftwerks für die Stromversorgung hätte.

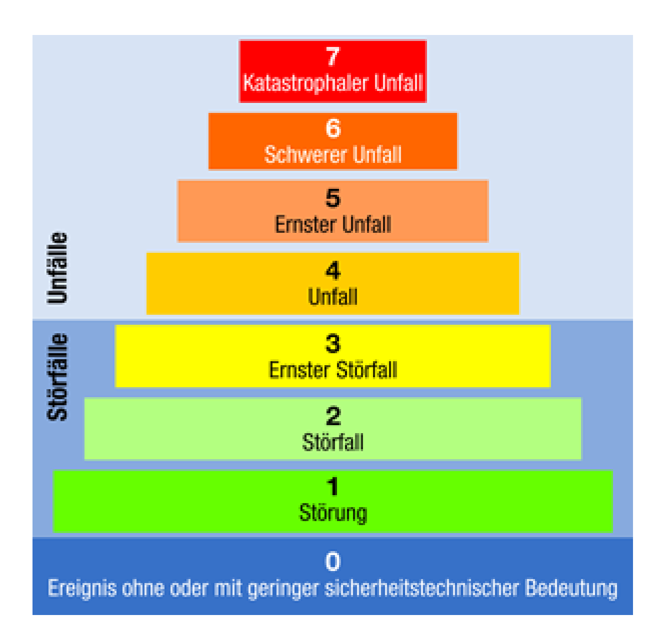



**Abbildung 12: INES – International Nuclear Event Scale**

Quelle: (GRS, o.J.)

Wie naheliegend dennoch ein terroristisches Szenario ist, zeigt ein vereitelter Bombenangriff auf den wichtigen Internetknotenpunkt *London Internet Exchange* im März 2006. Im Zuge kriminaltechnischer Untersuchungen wurden unter anderem auch Pläne für Attentate gegen Objekte wie Gasleitungen, Öllager oder Kommunikations-infrastrukturen entdeckt. Die Auswahl dieser Ziele zeigt, dass neben der ursprünglichen Intention terroristischer Anschläge – eine hohe Opferzahl zu erreichen – zunehmend das Kriterium *hoher wirtschaftlicher Schaden* in den Fokus der Handlungen gerät (MELANI, 2007, S. 24). Problematisch ist jedoch, dass Terroranschläge grundsätzlich



kaum vorhersehbar sind. Terroristen greifen meist überraschend an (Benzin, 2005, S. 222 f), weshalb eine genauere Aussage über das Gefahrenpotenzial fast unmöglich ist.

Außerdem kommen Experten zu dem Schluss, dass in den kommenden Jahren verstärkt mit Aktivitäten und neuen Angriffsmethoden zu rechnen ist, die auch als Cyberattacken bezeichnet werden (Reichenbach et al., 2008, S. 18). Diese Art von Kriminalität soll deshalb im Folgenden in einem Exkurs berücksichtigt werden.

### Exposition gegenüber Cyberattacken

Die hochgradige Vernetzung von Kritischen Infrastrukturen und Kritischen Informationsinfrastrukturen, die oftmals kaum getrennt zu betrachten sind, machen es in Zukunft notwendig, möglichen Cyberattacken besondere Beachtung zu schenken (Metzger, 2004). So argumentierte Otto Schily anlässlich einer Fachkonferenz für Kommunikationsforschung:

> *"[…] wir können leider nicht ausschließen, dass auch lebenswichtige IT-Infrastrukturen ins Visier terroristischer Anschläge rücken könnten. Innere Sicherheit ist daher heute untrennbar mit sicheren IT-Infrastrukturen verbunden. Die ständige Verbesserung der IT-Sicherheit ist zu einer festen Konstante unserer nationalen Sicherheitspolitik geworden. Es gibt keine innere Sicherheit ohne IT-Sicherheit"* (Schily, 2003).

Gemäß BSI (2009) ist seit einigen Jahren ein deutlicher Anstieg von Cyberattacken zu verzeichnen. Diese werden dabei von Möckli (2010) in fünf Dimensionen kategorisiert: *Cybervandalismus*, *Cyberhacktivismus*, *Internet-Kriminalität*, *Cyberspionage* und *Cyberwar* (siehe Abbildung 13). Diese Kategorisierung erfolgt nach dem potentiellen Schadensausmaß als Hauptunterscheidungsmerkmal, wobei die oberste Stufe, der Cyberwar auch den größten Schaden verursachen kann.



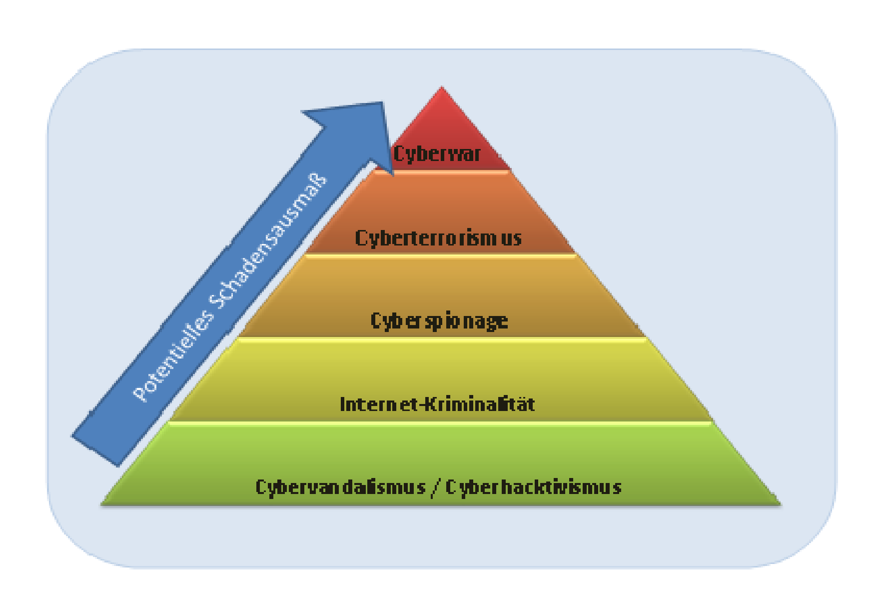



**Abbildung 13: Unterschiedliche Konfliktformen im Internet**

Quelle: (verändert nach Möckli, 2010, S. 2)

Auf der unteren Ebene befinden sich *Cybervandalismus* und *Cyberhacktivismus*. Bei *Cybervandalismus* handelt es sich um die Veränderung oder die Zerstörung von Internetinhalten oder dem Ausschalten von Webseiten durch Datenüberflutung. Diese Form von Cyberattacken ist die häufigste, zeitlich jedoch begrenzt und gilt im Vergleich zu den anderen Konfliktformen als harmlos, zumal sie nicht politisch oder wirtschaftlich motiviert ist (Möckli, 2010). Mit *Cyberhacktivismus* bezeichnet man ein politisch motiviertes *Hacken*, wobei Computer in unüblicher und häufig illegaler Form mit Hilfe spezieller Software manipuliert werden (Denning, 2001). In der Vergangenheit führten einzelne Software-Viren und –Würmer zu einem stark erhöhten Datenverkehr, der Teile der Internetinfrastruktur beeinträchtigte, sodass die Internetfunktionalität vereinzelt eingeschränkt war. In Folge dessen fielen beispielsweise Bankautomaten und Buchungssysteme von Fluggesellschaften aus (Kuhn, 2005, S. 12 ff). Fraglich ist, welche Auswirkungen Cybervandalismus und –hacktivismus auf die Stromversorgung haben können. Siehe hierzu auch die nachfolgende Textbox in diesem Kapitel.

Auf den nächsten beiden Stufen befinden sich die *Internet-Kriminalität* und die *Cyberspionage*, durch die überwiegend die Wirtschaft betroffen ist. Zu diesem Komplex zählen Netzwerkspionage zum Zwecke der Erpressung, Betriebsspionage, Onlinebetrug und andere Varianten des organisierten Betrugs. Der ökonomische Schaden belief sich im Jahr 2009 laut Bundeskriminalamt in Deutschland auf 37,2 Millionen Euro. KRITIS ist jedoch bisher kaum betroffen, auf eine entsprechende Gefährdungslage im Sinne einer theoretisch möglichen Erpressung deutscher Unternehmen aber auch staatlicher Institutionen wird hingewiesen (BKA, 2010).



Der *Cyberterrorismus* bezeichnet illegale Angriffe nichtstaatlicher Akteure gegen Computer und Computernetzwerke mit dem Ziel, einen Staat, eine Regierung und deren Bevölkerung einzuschüchtern und zu einer bestimmten Handlung oder Handlungsweise zu bewegen. Dies bedeutet, dass von Cyberterrorismus nur gesprochen werden kann, wenn der Angriff potentiell physische Schäden an Personen und oder Sachen bzw. schwere ökonomische Schäden verursachen könnte. Dies könnte insbesondere durch Angriffe auf KRITIS erreicht werden (Reichenbach et al., 2008; Fischer, 2007; Möckli, 2010).

Es ergibt sich die Möglichkeit über Schnittstellen mit dem Internet in sogenannte SCADA-Systeme (Supervisory Control and Data Aquisition-Systeme) einzudringen, und so die Kontrolle über diese zu übernehmen. Es handelt sich hierbei um Computersysteme, die Prozesse der physikalischen Infrastruktur steuern. Typische SCADA-Systeme beinhalten unter anderen folgende Komponenten:

- Instrumente zur Messung bestimmter Bedingungen in Anlagen, wie pH-Wert, Temperatur, Druck usw.
- Steuerungselemente für Geräte wie Pumpen, Ventile oder Förderanlagen
- Computer zur Prozessüberwachung, die beispielsweise Warnsignale ausgeben
- Kommunikationseinheiten zur Steuerung der lokalen Prozesse über Kabel- oder Funkverbindungen oder auch über Telefonleitungen oder Sattelitenverbindungen (Robles et. al, 2008).

Cyberterrorismus steht besonders im Mittelpunkt des Interesses, wenn es um eine Gefährdung von KRITIS geht, da das Internet geographische Hindernisse nebensächlich macht. So könnten Terroristen unabhängig von der Distanz Terrorpläne ausarbeiten und mit vermeintlich geringem finanziellen Aufwand und mit gegebenenfalls geringem Risiko Kritische Infrastrukturen zumindest für einen gewissen Zeitraum stören. Die Diskussionen, ob KRITIS durch Cyberorrismus gefährdet ist, wird kontrovers und zahlreich geführt (Fischer, 2007, S. 117-121).

Inwiefern ein Angriff auf KRITIS über SCADA-Systeme möglich sein könnte, ist umstritten und galt lange Zeit als unwahrscheinlich. Die zunehmende Vernetzung und Verknüpfung der ursprünglich autarken SCADA-Systeme mit dem Internet, erschließt Hackern jedoch zumindest die theoretische Möglichkeit der Manipulation oder Deaktivierung und somit der Schädigung physischer Elemente (Kuhn, 2005; Fischer, 2007). Die Komplexität und die Sicherheitsvorkehrungen der meisten SCADA-Systeme lässt erfolgreiche Angriffe unwahrscheinlich erscheinen. So sind bis vor kurzem keine ernsthaften Manipulationen oder Angriffe auf SCADA-Systeme durch Terroristen bekannt geworden. Einzelne Berichte, wie die Manipulation einer städtischen Wasserversorgung von Maroochy Shire in Queensland, Australien sind von einem entlassenen Angestellten, der sich über ein Funksystem illegal Zugang zu einem



Kontrollsystem verschafft hat, verursacht worden (Watts, 2003; Fischer, 2007; Kuhn, 2005). Seit letztem Jahr verdichten sich jedoch laut Frankfurter Allgemeine Zeitung (22. Sept. 2010) die Hinweise, dass der sogenannte *Stuxnet-Trojaner*[11] mit dem Ziel der verdeckten Installation einer Manipulationssoftware in einer Industrieanlage in Umlauf gebracht wurde. Das Schadprogramm ist so konzipiert, dass es unerkannt gezielt Veränderungen an den Einstellungen von Industrieanlagen vornehmen kann. Dies ist die bis dato erste beobachtete Cyberattacke auf ein SCADA-System, wobei bisher nicht klar ist, welcher Anlage dieser Angriff wirklich galt, wer die Schadsoftware in Umlauf brachte und mit welchem Ziel dieser „Angriff" durchgeführt wurde. Einzig aufgrund des enormen finanziellen[12] und technischen[13] Aufwands, mit dem dieser Trojaner erstellt wurde, sowie der für einen derartigen Angriff notwendigen Detailinformationen über die Anlagen, ist davon auszugehen, dass ein Angriff in dieser Größenordnung nur von einem Nationalstaat – Kategorie Cyberwar siehe Abbildung 13 – ausgeführt werden kann. Aufgrund der hohen Infektionsrate durch den Trojaner im Iran, sowie weiteren Hinweisen gehen Experten davon aus, dass der Angriff einer iranischen Urananreicherungsanlage galt. Besonders die Identifikation des Urhebers, sowie das eigentliche Ziel des Angriffs bleiben weiter im Unklaren.[14]

Hinsichtlich des Zwischenfalls im Iran könnte sich zukünftig eine weitere Gefährdung für Kritische Informationsinfrastrukturen entwickeln, die als *Cyberwar* bezeichnet wird. Diese wäre ein Teil einer Informationskriegsführung mit dem Ziel eigene Informationsinfrastrukturen zu schützen und die des Gegners zu stören. Der Cyberwar hätte ein enormes Schadenspotential für KRITIS und somit für die Sicherheit und Wohlfahrt des Staates. Aktuell erscheint ein Szenario eines Cyberwars, eines nur noch im Informationsraum ausgetragenen zwischenstaatlichen Konflikts, kaum realistisch. Der Zwischenfall im Iran zeigt jedoch, mit welchen Angriffen möglicherweise in Zukunft zu rechnen ist (Reichenbach et al., 2008; Fischer, 2007; Möckli, 2010).

Neben dem Szenario eines Cyberwars birgt das, aufgrund der Systemumstellung computerisierte Stromnetz, in Zukunft vermehrt Sicherheitsrisiken. Durch die untereinander vernetzten, computergesteuerten Smart Meter (siehe Kapitel 6.3.3) sind sowohl Verbraucher als auch die gesamte Infrastruktur verwundbar gegenüber Cyberattacken (McDaniel & McLaughlin, 2009). Gleichzeitig zeigt eine aus Sicherheitsgründen unveröffentlichte Studie des Sicherheitsbereatungsunternehmens IOActive, dass die neue Technologie (Smart Grids) sehr anfällig gegenüber Hackern ist und folglich die

[11] Trojaner sind kleine Schadsoftware-Programme, die verdeckt die Kontrolle über einen Computer übernehmen können (BSI, 2009).

[12] Vermutet werden Kosten im siebenstelligen Euro-Bereich (Rieger, 2010).

[13] Die Qualität und Durchschlagskraft der Angriffsmethode des „Stuxnet-Trojaners" ist bis dato neuartig (Rieger, 2010).

[14] Jede Industrieanlage ist in der Zusammenstellung der Einzelkomponenten individuell, weshalb die Angreifer über hochpräzise Informationen zum Aufbau der Anlage verfügen müssen (Rieger, 2010).



Stabilität des gesamten Stromnetzes gefährdet ist (Sam, 2009). Laut Sicherheitsexperten kann eine Manipulation des comuptergesteuerten Smart Grid-Netzwerks mit geringem finanziellen und technischen Aufwand von jedem Computer aus zu einem großflächigen Ausfall führen (McDaniel & McLaughlin, 2009). Besonders im Zuge der Systemumstellung sind derartige Erkenntnisse von großer Relevanz für zukünftige Sicherheitsmaßnahmen.

**Beispiel: Cyberattacken auf Estland**

Als ein Beispiel für eine *Cyberattacke* auf KRITIS kann der Angriff Ende April 2007 auf Estland gelten. Nachdem eine Webseite ein Softwareprogramm zur Durchführung von DoS Attacken[1] auf estnische Internetseiten zur Verfügung gestellt und zu Angriffen aufgerufen hatte, erfolgten diese mit bisher nicht beobachteter Konzentration auf offizielle estnische Internetseiten. Erklären lässt sich dies mit dem Abbau sowjetischer Kriegsdenkmäler in Estland durch die dortigen Behörden, die sogar die russiche Regierung hinter den Attacken vermuteten. Einzelne Angriffe dauerten bis zu 11 Stunden und verteilen sich auf den Zeitraum vom 28. April bis zum 11. Mai 2007 (Alvaro, 2009). Der Datenverkehr stieg in diesem Zeitraum um 400% im Vergleich zur normalen Datenlast. Bereits kurz nach Beginn des Angriffs waren die Webseiten des estnischen Präsidenten, des Premierministers, des Parlaments und zahlreicher Ministerien nicht erreichbar. In den folgenden Tagen weiteten sich die Angriffe auf estnische Internet Service Provider, Mailserver, Online-Banken und andere Internetdienste aus. Der wirtschaftliche Schaden der Attacke wurde mit 10 Millionen US Dollar geschätzt (MELANI, 2007; Alvaro, 2009; Dunham & Melnick, 2009)

Der estische Verteidigungsminister Jaak Aaviksoo resümierte:

> *„I tend to term the events that took place in Estonia earlier this year as cyber-terrorism.”* Dunham & Melnick, 2009).

Besonders interessant an dem Beispiel des Angriffs auf Estland ist der Umstand, dass Estland zu den informationstechnisch am weitesten entwickelten Ländern gehört. So ist die Internetnutzung landesweit kostenlos, und es besteht eine nahezu landesweite WLAN-Abdeckung. Offensichtlich geht der Fortschritt in diesem Bereich mit einer erhöhten Verwundbarkeit einher (Alvaro, 2009).

---------

[1] Denial of Service (DoS) Attacken sind in aller Regel Angriffe auf einen vernetzten Computer durch Überlastung. Ein bestimmter Dienst (z.B. HTTP) wird mit einer überaus großen Anzahl von Anfragen belastet, so dass eine Bearbeitung nicht mehr möglich ist. Eine besondere Form stellen die oben beschriebenen DDoS-Attacken (Distributed Denial of Service Attacken) dar. Mitels einer speziellen Software wird der Angriff von vielen Computern gleichzeitig (ein „Botnetz“ wird aufgebaut) durchgeführt (Saafan, 2009; Alvaro, 2009).

### 4.1.3 Übersicht einiger Stromausfälle

Im Folgenden soll nun auf einige Beispiele von Stromausfällen eingegangen werden (siehe Tabelle 4), um exemplarisch zu veranschaulichen, wie Naturgefahren aber auch menschliches Versagen dazu führen können, dass es zu weitreichenden negativen Auswirkungen in der Stromversorgung kommt.



**Tabelle 4: Überblick ausgewählter Stromausfälle**

| Datum | Land / Region | Ursache | Auswirkungen |
|---|---|---|---|
| 14. 08. 2003 | Nordosten der USA/ Zentralkanada | Mehrere zufällige Kraftwerksausfälle, hohe Netzbelastung bereits im Normalbetrieb, mangelnde Kommunikation und Koordination zwischen den Netzbetreibern | Stromausfall: ca. 50-60 Mio. Menschen ohne Strom Dauer: zwischen 4 und 48 Stunden |
| 28. 08. 2003 | Großbritannien/ London | Geschwächte Netzinfrastruktur durch wartungsbedingte Abschaltungen in Verbindung mit zwei Störfällen | Stromausfall: ca. 500.000 - 1 Mio. Menschen ohne Strom Dauer: 35 Minuten |
| 23. 09. 2003 | Schweden/Dänemark | Zusammenwirken planmäßiger Abschaltungen und zeitnahes Eintreten von zwei Störfällen | Stromausfall: ca. 3,8 - 5 Mio. Menschen ohne Strom Dauer: etwa 6,5 Stunden |
| 28. 09. 2003 | Italien/Schweiz | Überhöhter Stromimport über die Schweiz nach Italien führte zu Schäden und zum Ausfall von Transitleitungen | Stromausfall: ca. 57 Mio. Menschen für eine Dauer von bis zu 20 Stunden |
| 02. 09. 2004 | Deutschland/ Luxemburg | Fehlerhafte 220-kV-Leitung, Wartungsarbeiten und eine verfrühte Überlastungsauslösung | Blackout im Raum Trier und Luxemburg, etwa 540.000 Betroffene. Dauer: bis zu 4:40 Stunden |
| 13. 05. 2005 | Frankreich | Waldbrand erforderte das Abschalten von zwei Hochspannungsleitungen | Über 1 Mio. Haushalte in Südfrankreich waren für mehrere Stunden ohne Strom |
| 25. 11. 2005 | Deutschland/ Münsterland | Starke Eisbildung an Freilandleitungen führten zur Zerstörung von Leitungen und Strommasten | Stromausfall für bis zu 250.000 Menschen für die Dauer von bis zu 5 Tagen |
| 27. 03. 2006 | Deutschland/ Hamburg | Unwetter/Tornado: Beschädigungen an Freileitungen führten zu Kurzschlüssen im 380-kV-Übertragungsnetz | Stromausfall für 300.000 Menschen für fast 12 Stunden |
| 04. 11. 2006 | Westeuropa/ Deutschland | Abschaltung einer Doppelleitung ohne Einhaltung der Sicherheitskriterien, mangelnde Kommunikation und Koordination der Netzbetreiber | Kaskaden-Kollaps: Blackout in Deutschland, Frankreich, Italien, Belgien, Spanien, Portugal; etwa 10 Mio. Menschen betroffen; Zerfall des UCTE-Verbundes in drei Teilnetze; Dauer: etwa 37 Minuten |
| 30. 01. 2008 | Deutschland/ Karlsruhe | Brand eines 110 kV-Messwandlers führte zur automatischen Abschaltung von Einspeisungstransformatoren | Stromausfall im gesamten Stadtgebiet Karlsruhe für einen Zeitraum von bis zu 74 Minuten. |

(grau hinterlegt) Diese Beispiele werden noch ausführlicher beschrieben.

Quelle: eigene Darstellung nach (Tagwerker, 2004; CONSENTEC et al., 2008; Bundesnetzagentur, 2007; Bundesnetzagentur, 2006a; EnBW, 2008; Thierauf, 2006; Schossing, 2007; Bacher & Näf, 2003).



Schweden/Dänemark

Etwa 3,8 Millionen Schweden und Dänen waren am 23.09.2003 von einem Stromausfall betroffen. Dieser umfasste die Region Kopenhagen/Malmö sowie den südlichen Teil Schwedens bis etwa 150 km südlich von Stockholm. Des Weiteren waren die Inseln Seeland, Bornholm und Lolland-Falster ohne Strom. In Folge dieses Ereignisses fielen Ampelanlagen aus, der Bahnverkehr mussten eingestellt werden, die Brücke zwischen Malmö und Kopenhagen wurde geschlossen und der Flughafen Kopenhagen-Kastrop musste vorübergehend seinen Betrieb einstellen.

Die Ursachen hierfür waren vielfältig. So war zunächst das Kernkraftwerk Oskarshamm wegen eines Ventilproblems im Kühlwasserkreislauf abgeschaltet worden und auch die Seekabelverbindungen nach Deutschland und Polen waren wartungsbeding abgeschaltet. Nahezu gleichzeitig ereignete sich ein unabhängiger Fehler im Umspannwerk „Horred“, der zum Ausfall von zwei Reaktorblöcken des KKW „Ringhals“ führte. Dies bedingte schließlich einen Spannungszusammenbruch im gesamten Netz südwestlich von Stockholm. Nach etwa 6,5 Stunden wurde die Stromversorgung weitgehend wieder hergestellt, nachdem das Netz von Wasserkraftwerken Norwegens, Nordschwedens und Finnlands unterstützt und begonnene Wartungsarbeiten abgebrochen worden waren (CONSENTEC et al., 2008; Tagwerker, 2004; Schossing, 2007).

Italien/Schweiz

Am 28.09.2003 fiel in ganz Italien und kurzzeitig in Teilen der Schweiz der Strom aus. Insgesamt betraf der Ausfall etwa 57 Millionen Menschen. In der Nacht fand in Rom die „Weiße Nacht“ statt, die Museen der Stadt hatten die gesamt Nacht über kostenlos geöffnet, es fanden zahlreiche Kulturveranstaltungen statt. Der hieraus resultierende erhöhte Strombedarf in Italien führte in den frühen Morgenstunden zu einem überhöhten Stromimport über die Transitleitungen der Schweiz in Höhe von etwa 300 MW. Daraufhin fiel eine 380-kV-Leitung aufgrund der Überlastung aus und konnte nicht wieder eingeschaltet werden. Der zu transportierende Strom wurde auf die ohnehin stark ausgelasteten Leitungen verteilt. Innerhalb von ca. 30 Minuten fiel eine weitere Transitleitung in der Schweiz aus. Die starke Belastungszunahme auf den verbleibenden Leitungen führte zu kaskadenartigen Abschaltungen, die Italien schließlich vollständig vom übrigen Netz der *Union für die Koordinierung des Transports von Elektrizität* (UCTE-Netz) trennte. Das italienische Netz konnte wegen des erheblichen Energiedefizits nicht im Inselbetrieb aufrecht erhalten werden, es kam zu einem vollständigen Blackout in ganz Italien. Auch in der Schweiz gab es regionale Stromausfälle bis zu 1 ½ Stunden. Norditalien konnte nach wenigen Stunden wieder aus dem UCTE-Verbund heraus versorgt werden, Rom ab Mittag und im Süden des Landes



erfolgte die Wiederaufnahme nach etwa 20 Stunden (CONSENTEC et al., 2008; Tagwerker, 2004; Schossing, 2007; Bacher & Näf, 2003).

Trier/Luxemburg

Am 02.09.2004 kam es auf einer 220-kV-Leitung „Saar-Nord“ zu einem Kurzschluss zwischen zwei Leiterseilen, deren Ursache nicht zu ermitteln war. Gleichzeitig wies ein Schutzgerät der 220-kV-Leitung „Osburg“ eine Überfunktion aus, das diese automatisch abschaltete. Auch fanden Wartungsarbeiten an einem Kuppeltransformator in der Nähe von Bitburg statt. Nach dem Ausfall der beiden 220-kV-Leitungen wurde die 220-kV-Leitung „Kondelwald“ wegen der nun erheblichen Überlast automatisch vom Netz genommen.

Das gesamte 220-kV-Netz in der Region Trier und in Luxemburg war um 16:51 Uhr spannungslos, der Leistungsausfall betrug auf deutscher Seite etwa 380 MW, in Luxemburg etwa 480 MW. Vor Eintreten der Störung befand sich das Netz trotz ausgeschaltetem Transformator in einem sicheren Zustand, da das Kraftwerk „Vianden“ mit einem Zwangseinsatz das Netz mit etwa 200 MW stützte. Die Aufnahme des Pumpspeicherkraftwerks Vianden erforderte eine Leistungsaufnahme von 68 MW. Eine Sicherheitsrechnung nach erfolgter Störung hätte ergeben, dass die Netzsicherheit gefährdet ist, was einen Ausfall verhindert hätte. Wäre eine geplante aber noch nicht erfolgte Installation eines zweiten Netzkuppeltransformators bereits fertiggestellt gewesen, wäre es ebenfalls nicht zu den Stromausfällen gekommen.

Nachdem Teile des Netzes in Luxemburg über Belgien versorgt wurden und die abgeschalteten Leitungen nach Inspektionen der ausgefallenen Leitungen wieder hinzugeschaltet worden waren, waren alle 220-kV-Leitungen wieder unter Spannung, so dass der Normalbetrieb des 220-kV-Netzes in Luxemburg gegen 17:23 Uhr wieder hergestellt werden konnte. Da Verteilungsnetztransformatoren in Trier und der Eifel für eine Zuschaltung vorbereitet werden mussten und gemäß eines RWE Netzwiederaufbaukonzeptes vor Ort von Hand mit Hilfe einer Ortssteuerung in den Umspannungsanlagen zu regeln waren, war die Wiederversorgung aller Kunden erst ab 21:24 Uhr möglich. Der Stromausfall betraf insgesamt etwa 540.000 Menschen. Nachdem RWE die Ursache für die Kurzschlüsse nicht ermitteln konnte und Zeugen unabhängig voneinander den Verdacht äußerten, dass die Kurzschlüsse durch Fremdverschulden verursacht worden waren, stellte RWE bei der Staatsanwaltschaft Saarbrücken Strafanzeige gegen unbekannt (CONSENTEC et al., 2008, S. 134 ff; Schossing, 2007).

Deutschland/Münsterland

In der Nacht vom 25.11.2005 kam es zu schwerem Schneefall im Münsterland. Das Zusammenspiel mehrerer Schadensauslöser gleichzeitig (u.a. sehr starker Wind, extremer Schneefall, Temperaturen um 0° C, sehr nasser Schnee mit hohem Gewicht,



zeitweise einsetzender Regen und ungünstige Windrichtung) ließ Stromleitungen reißen und Strommasten brechen, sodass innerhalb kürzester Zeit sieben 110-kV-Freileitungsstrecken ausfielen. Etwa 250.000 Menschen im westlichen Münsterland wurden von der Stromversorgung abgeschnitten. Trotz des Einsatzes von bis zu 400 Beschäftigten eines RWE-Reparaturtrupps dauerte es bis zu 120 Stunden, bis die Stromversorgung in der gesamten Region wiederhergestellt werden konnte. Notstromaggregate wurden aus dem ganzen Bundesgebiet eingeflogen, um verderbliche Waren zu kühlen oder auf Bauernhöfen Melkstände betreiben zu können. Der insgesamt entstandene Schaden belief sich laut IHK Münster auf etwa 100 Millionen Euro, RWE schätzte den eigenen Schaden auf 35 Millionen Euro.

Aufgrund angeblicher Sicherheitsmängel und eines Sanierungsbedarfs des betroffenen Netzes wurde der Betreiber RWE von der Politik auf Landes- und Bundesebene aufgefordert, Stellung zu nehmen. Darauf folgende Gutachten und ein Untersuchungsbericht der Bundesnetzagentur kamen zu dem Ergebnis, dass die witterungsbedingte Überbelastung ursächlich für die Mastbrüche war und nicht etwa eine durch mangelnde Pflege entstandene Korrosion der Stahlkonstruktionen. Der Netzbetreiber wies darauf hin, dass die nach der gültigen VDE-Vorschrift[15] zulässige Gewichtsbelastung um das 8- bis 15-fache überschritten worden war. Wegen der anhaltenden Kritik an Stahlmasten und Stahlkonstruktionen aus *Thomasstahl*, welche mit zunehmendem Alter an Elastizität verlieren würden, hat sich RWE dennoch entschlossen, bis zum Jahr 2015 etwa 28.000 betroffene Strommasten zu ersetzen. Die Ereignisse im Münsterland waren für die Politik Anlass, die Sicherheit von Stromnetzen anderer Regionen und Bundesländer zu überprüfen[16] (CONSENTEC et al., 2008, S. 136 f; Thierauf, 2006; Bundesnetzagentur, 2006).

<u>Deutschland/Westeuropa</u>

Um einem Kreuzfahrtschiff aus Papenburg eine gefahrlose Überführung zu ermöglichen, entschied sich die E.ON Netz GmbH am Abend des 04.11.2006 um 21:38 Uhr eine Höchstspannungsleitung über der Ems abzuschalten. Eine vorangegangene Simulationsrechnung wies laut E.ON nicht darauf hin, dass die Netzsicherheit gefährdet sein könnte. Unmittelbar nach der erfolgten Abschaltung liefen mehrere Warnmeldungen wegen des Erreichens von Stromgrenzwerten auf. E.ON sah hier keinen Handlungsbedarf, da die vorhandenen freien Netzkapazitäten für eine temporäre Überlastung als ausreichend angesehen wurden. Ein Gespräch zwischen E.ON und RWE ergab um 21:41 Uhr, dass die Leitung „Landsbergen-Wehrendorf“, welche beide Netzbetreiber verbindet, einen Sicherheitsgrenzwert von 1800 Ampere (A) aufwies. Zu diesem Zeitpunkt belief sich die Belastung der Leitung auf etwa 1780 A. Innerhalb

[15] DIN VDN 0210/85

[16] Vgl. Landtag von Baden-Württemberg: Antrag der Fraktion GRÜNE und Stellungnahme des Wirtschaftsministeriums Sicherheitsmängel bei Strommasten des baden-württembergischen Freilandleitungsnetzes vom 6.12.2005.



weniger Minuten stieg die Belastung der Leitung um ca. 160 A, ohne dass die Ursache bekannt war. Um 22:07 Uhr stellten E.ON und RWE fest, dass Sicherheitsgrenzwerte überschritten wurden und dass Maßnahmen zur Errichtung eines sicheren Netzbetriebes notwendig waren. Korrektive Maßnahmen im Umspannwerk Landesbergen durch E.ON wurden ohne vorherige Netzsicherheitsrechnung und ohne Abstimmung mit RWE durchgeführt. Um 22:10 Uhr wurde die Leitung „Landsbergen-Wehrendorf“ von einer automatischen Schutzeinrichtung wegen Überlastung abgeschaltet. Die nun erfolgten Lastverschiebungen bedingten kaskadenartig weitere Abschaltungen von Übertragungsleitungen in Richtung Süden und verursachten schließlich ein Auseinanderfallen des gesamten europäischen UCTE-Netzes in drei Teilnetze (vgl. Abbildung 14).

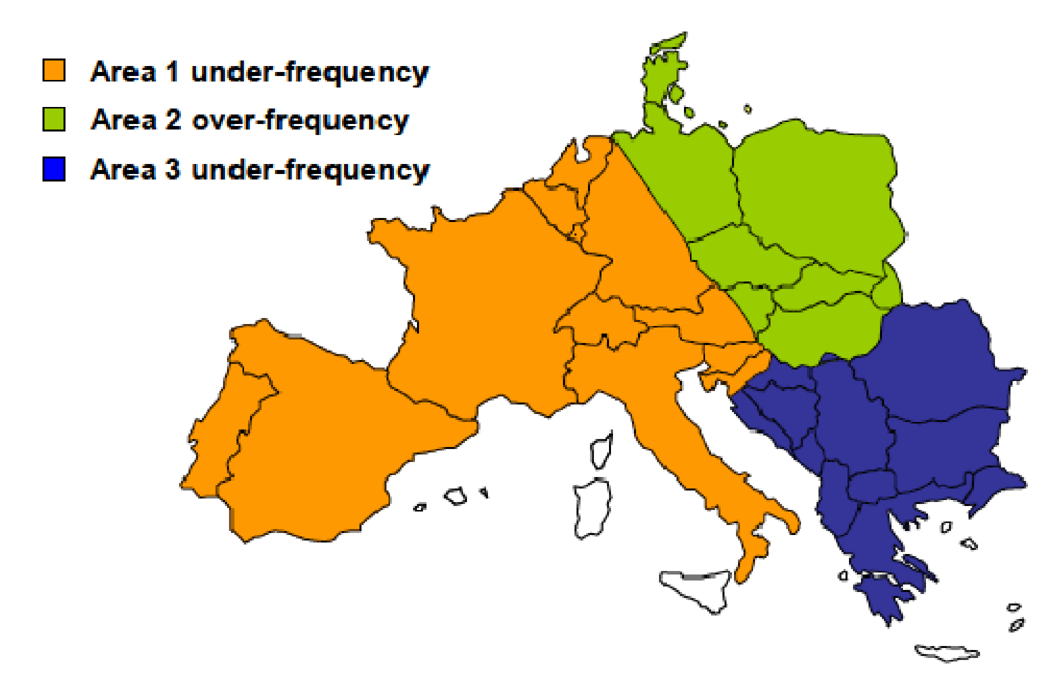



**Abbildung 14: Schematische Teilung des UCTE Netzes in drei Gebiete**

Quelle: (UCTE, 2007, S. 21)

Im nordöstlichen Teil kam es wegen eines Energieüberschusses zu einem Frequenzanstieg, der durch eine Verringerung der Einspeiseleistung ausgeglichen wurde. In den beiden unterversorgten Gebieten mussten kontrollierte Abschaltungen von Industrie- und Haushaltskunden vorgenommen werden, da es sonst zu unkontrollierten Blackouts in den unterversorgten Teilnetzen gekommen wäre. Ab 22:47, etwa 37 Minuten nach Eintreten der ersten Störung, konnten die Teilnetze wieder synchronisiert und verbunden werden.

Als zusätzliche Ursache des Ausfalls wurde die fluktuierende Energieeinspeisung durch Windenergie angeführt. Der Abschlussbericht der Bundesnetzagentur kommt jedoch zu dem Schluss, dass es zum Zeitpunkt der Störung keine nennenswerte Belastung durch



Windenergie gab. Eine Überlastung der Leitung „Landesbergen-Wehrendorf“ durch Windenergie wurde ausgeschlossen, da sich die Windkraftanlagen weitestgehend und planmäßig automatisch vom Netz getrennt hatten, was den Erzeugermangel in einigen ohnehin unterversorgten Gebieten zusätzlich verschlimmerte. In dem Teilgebiet mit zu hoher Netzlast schalteten sich die Windkraftanlagen außerdem zum Teil zu früh zu, was die Stabilisierung und Resynchronisierung der Netzgebiete erschwerte. Konventionelle Kraftwerke in der Region des Netzbetreibers Vattenfall Europe Transmission konnten nicht weiter heruntergefahren werden, da diese bereits im Erzeugerminimum betrieben wurden. Der entstandene Überschuss konnte erst durch Abschalten polnischer Kraftwerke kompensiert werden. Eine Stabilisierung der Netzgebiete wurde dadurch erschwert, dass die Übertragungs- und Verteilnetzbetreiber weder Kontrolle über die automatische Wiedereinschaltung der Windkraftanlagen noch Echtzeitinformationen über die dezentralen Erzeugungseinheiten hatten (CONSENTEC et al., 2008; van der Vleuten & Lagendijk, 2010; Bundesnetzagentur, 2007).
Die Bundesnetzagentur wies darauf hin, dass es Pflicht des Netzbetreibers sei, die Netzsicherheit jederzeit zu gewährleisten. Gegen diese Regel wurde verstoßen. Des Weiteren stellt die Bundesnetzagentur fest, dass ein Ausbau der Netzinfrastruktur zur Sicherstellung des (n-1)-Kriteriums notwendig ist (Bundesnetzagentur, 2007, S. 30; Kurth, 2006; 2005).

Karlsruhe

Am 30. Januar 2008 führte ein Brand in einem Trafogebäude zu einem Kurzschluss. Dieser verursachte in Karlsruhe-West und Karlsruhe-Ost eine automatische Abschaltung von drei Transformatoren, die im Normalbetrieb die Stromspannung von 220 kV auf 110 kV herunter transformieren und in das Stromnetz der Stadt speisten. In Folge dieses Ereignisses kam es um 17:36 Uhr zu einem vollständigen Blackout in der Stadt Karlsruhe. Nach entsprechenden Maßnahmen im Umspannwerk Ost konnte ein Großteil des Stadtgebiets ab 17:53 Uhr wieder mit Strom versorgt werden. Nach Abschluss der Löscharbeiten im Umspannwerk West konnten ab 18:50 Uhr alle Haushalte wieder mit Strom versorgt werden (EnBW, 2008).

### 4.1.4 Zwischenfazit Exposition

Deutschland mit seinen unterschiedlichen Regionen und die in ihnen vorhandene KRITIS sind gegenüber einer Reihe unterschiedlicher Naturgefahren exponiert. Allerdings sind nur wenige Naturgefahren wie beispielsweise Sturmfluten und Hochwasser räumlich einzugrenzen. Auch variiert die Möglichkeit je nach Naturgefahr eine Vorhersage und dadurch Vorbereitungen zu treffen. Ferner ist der Klimawandel mit seinen Auswirkungen zu beachten, der auch in Deutschland zu bemerken ist. Eine naturräumliche Gliederung Deutschlands ergibt daher folgende Tendenzen für die



verstärke Exposition gegenüber bestimmten Naturgefahren in unterschiedlichen Regionen mit ihrer KRITIS:

- *Ostdeutschland*: Hier liegt eine hohe Exposition gegenüber Dürren vor. Diese können durch den Klimawandel weiter verstärkt werden. Im Einzugsgebiet von Elbe und Oder besteht zudem ein hohes Hochwasserrisiko.
- *Südwestdeutschland:* Hier sind schon heutzutage die Höchstwerte in Deutschland anzutreffen, und hier wird – bedingt durch den Klimawandel – mit den stärksten Temperaturanstiegen gerechnet. Daraus folgt die Exposition gegenüber Hitzewellen. Außerdem ist die Region gegenüber Hochwassern exponiert.
- *Mittelgebirge:* Durch ein eher kühles, feuchtes Klima kann in dieser Region eine mögliche Klimaerwärmung eher ausgeglichen werden. Dennoch besteht auch in der Region Mittelgebirge eine Exposition gegenüber Hochwassern, welche durch konvektive Starkniederschläge ausgelöst werden können.
- *Küstengebiet:* Hier liegt eine Exposition gegenüber dem tendenziellen Anstieg des Meeresspiegels sowie eventuell intensiveren Sturmfluten vor.

Die Auswirkungen der jeweiligen Naturgefahr auf die Elektrizitätsversorgung ist zudem unterschiedlich. Während die Störung der Elektrizitätsversorgung bei einem Hochwasser vielfach auf das Überschwemmungsgebiet beschränkt ist, kann es bei einer Hitzewelle zu überregionalen Auswirkungen kommen. Auch sind oberirdische Komponenten stärker exponiert als unterirdische (oberirdische Leitungen vs. Erdkabel). Die Störung des Stromnetzes hängt schließlich davon ab, welche Komponenten und Prozesse beschädigt sind. Je nach Stellung der beeinträchtigten KRITIS sind unterschiedlich große Gebiete von der Störung der Stromversorgung betroffen.

Neben den Naturgefahren sind jedoch insbesondere seit den terroristischen Anschlägen in den USA und Europa auch Kritische Infrastrukturen in Deutschland in den Fokus staatlicher Sicherheitsbemühungen gerückt. Besonders Kernkraftwerke gelten als Zielobjekte mit verheerenden Folgen für das Umfeld. Jedoch ist die Bedeutung ihres möglichen Ausfalls für die Stromversorgung aufgrund ihres relativ geringen Anteils an der Bruttostromerzeugung unklar.

Des Weiteren ist die Stromversorgung auch Angriffen mittels des Internets exponiert. So stellen insbesondere Schnittstellen mit dem Internet Einfallstore für Hacker auf SCADA-Systeme dar, die so zumindest theoretisch und in Teilen die Kontrolle der Stromversorgung übernehmen können. Unklar bleibt jedoch, ob die beschriebenen Schwächen des Internets selbst und der hierüber verknüpften SCADA-Systeme sich tatsächlich eignen, um großflächig terroristische Angriffe durchzuführen. Jedoch zeigen jüngste Ereignisse im Iran, dass mit einem solchen Angriff gerechnet werden muss.



Auch bleibt abzuwarten, wie sich die Einführung neuer Technologien, wie beispielsweise der Smart Grids, auf Cyberattacken auf die Stromversorgung auswirken werden.

Ein Überblick über ausgewählte Stromausfälle der Vergangenheit zeigt jedoch, dass zumeist nicht ein einzelnes und eindeutig zurechenbares Ereignis, wie beispielsweise bestimmte Naturgefahren oder Angriffe, zur Störung führte. Zumeist kommt es zu Großstörungen, wenn unterschiedliche Schadensereignisse, wie beispielsweise gleichzeitige Kraftwerks- und Leitungsausfälle, zusammentreffen. Insbesondere bei Nichteinhaltung von Sicherheitsregeln wie der Verletzung des (n-1) Kriteriums, ist die Netzsicherheit nicht gegeben, sodass es zu großflächigen und länger dauernden Blackouts kommen kann. Bei Netzausfällen ist oftmals ein unzureichender Informationsaustausch zwischen den unterschiedlichen Übertragungsnetzanbietern oder Verteilungsnetzanbietern zu beobachten, der die Netzsicherheit gefährdet und somit Stromausfälle begünstigt. So kann es etwa bei planmäßigen Abschaltungen oder Wartungsarbeiten ohne hinreichende Sicherheitsrechnung oder Rücksprache mit allen betroffenen Stellen, insbesondere in Verbindung mit nicht vorhersehbaren Schadensereignissen, in einem hochgradig komplexen System wie dem Stromnetz, zu schwer kontrollierbaren, kaskadenartigen Netzausfällen kommen. Diese Effekte werden bei einer hohen Netzauslastung entsprechend verstärkt.

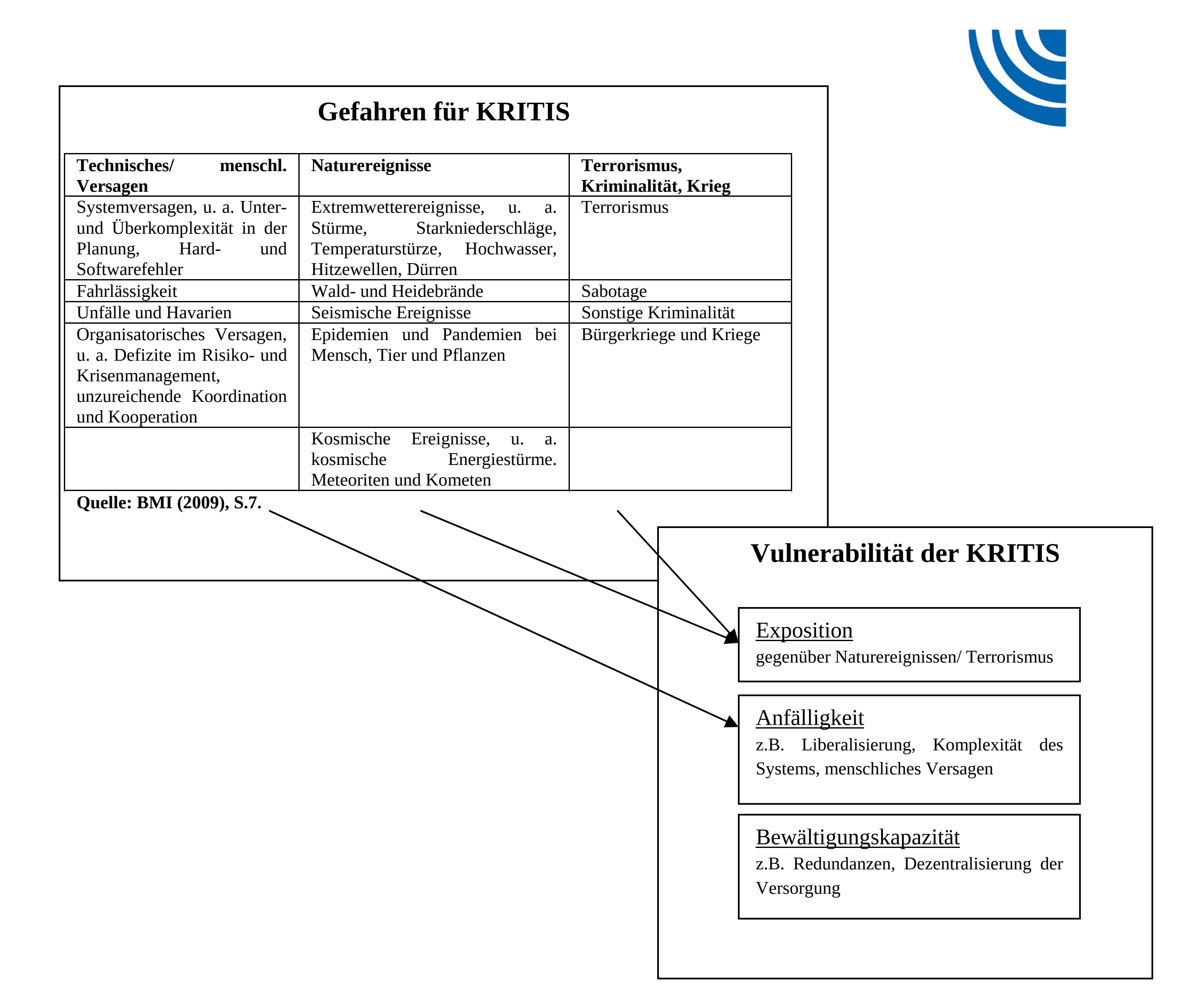


## 4.2 Anfälligkeit

Nachdem in Kapitel 4.1 die Gefahren analysiert worden sind, denen gegenüber die Kritische Elektrizitätsinfrastruktur verwundbar sein kann, werden im folgenden Teil die Faktoren näher beschrieben, die sich auf die Anfälligkeit der KRITIS auswirken:

| f (Vulnerabilität) = Exposition (Gefahr), **Anfälligkeit**, Bewältigungskapazität |
|---|

Weil die Anfälligkeit der Elektrizitätsinfrastruktur, wie eingangs beschrieben, nicht mithilfe des bestehenden Konzepts von Krings (in Druck) beschrieben werden kann, da hier kein spezifisches Gefahrenszenario verwendet wird, sondern eher genereller auf die Anfälligkeit von KRITIS im Zusammenhang zahlreicher Gefahren eingegangen werden soll, wird auf den Ansatz von Kröger (2008) zurückgegriffen. Kröger (2008, S. 1783) skizziert verschiedene Kategorien, die die Anfälligkeit von Kritischer Elektrizitäts-infrastruktur beeinflussen können: u. a. institutionelle, gesellschaftliche, system-bezogene und technologische Faktoren, die im Folgenden eingehender thematisiert werden. Zudem sollen menschliche Faktoren analysiert werden, die, ebenso wie die technologischen Faktoren, vom BMI (2009) unter dem Punkt *technisches/menschliches Versagen* zusammengefasst werden. Er gilt als eine der Ursachen, die zu Störungen oder Ausfällen von KRITIS führen können. Im Gegensatz zu *Naturereignissen* und *Terrorismus, Kriminalität* oder *Krieg* muss das technische/menschliche Versagen nämlich, wie in Abbildung 15 dargestellt, nicht als potenzielle Gefahr, sondern als systeminterne Eigenschaft verstanden werden (also eher der Anfälligkeit des Systems zugeordnet werden). Das System der Elektrizitätsversorgung ist diesen Ereignissen gegenüber nicht ausgeliefert, sondern kann sie vielmehr selber beeinflussen. Dieses Verständnis ist für die Entwicklung möglicher Strategien zur Verminderung der Verwundbarkeit von entscheidender Bedeutung, denn die Qualität und Verlässlichkeit von Technik sowie die Ausbildung und Verfassung der Mitarbeiter sind Bereiche, die durch gezielte Maßnahmen verbessert werden können. Zudem wird damit einem integrativeren Verständnis von Verwundbarkeit Rechnung getragen, dass neben der Exposition (Gefahr von Außen), auch die Anfälligkeit des Systems selbst (system-interne Faktoren) und die Bewältigungskapazitäten (z.B. Kapazitäten der Mitarbeiter) in den Mittelpunkt der Betrachtung rückt.




| Technisches/ menschl. Versagen | Naturereignisse | Terrorismus, Kriminalität, Krieg |
|---|---|---|
| Systemversagen, u. a. Unter- und Überkomplexität in der Planung, Hard- und Softwarefehler | Extremwetterereignisse, u. a. Stürme, Starkniederschläge, Temperaturstürze, Hochwasser, Hitzewellen, Dürren | Terrorismus |
| Fahrlässigkeit | Wald- und Heidebrände | Sabotage |
| Unfälle und Havarien | Seismische Ereignisse | Sonstige Kriminalität |
| Organisatorisches Versagen, u. a. Defizite im Risiko- und Krisenmanagement, unzureichende Koordination und Kooperation | Epidemien und Pandemien bei Mensch, Tier und Pflanzen | Bürgerkriege und Kriege |
| | Kosmische Ereignisse, u. a. kosmische Energiestürme. Meteoriten und Kometen | |



**Abbildung 15: Übertragbarkeit der Ursachen für Stromausfälle in das Konzept der Vulnerabilität**

Quelle: (eigene Darstellung, siehe auch BMI, 2009, S.7)

## Institutionelle Faktoren

Ein Faktor, der die Anfälligkeit der Kritischen Elektrizitätsinfrastruktur beeinflusst, ist die *Kapazität des Netzes und seine Auslastung*. Gemäß der UCTE (heute Mitglied des European Network of Transmission System Operators for Electricity, ENTSO-E), arbeitet das Europäische Verbundnetz immer mehr an seinen Kapazitätsgrenzen. Dies liegt insbesondere daran, dass viele Kritische Infrastrukturen in einer Größenordnung und Art und Weise operieren müssen, für die sie ursprünglich nicht geplant waren. So wurde das westeuropäische Elektrizitätsnetz mit seinen vertikal integrierten Komponenten (siehe Abbildung 4 auf Seite 10) für den jeweils nationalen Bedarf konstruiert. Im Rahmen der Integration der europäischen Staaten innerhalb der EU und der politisch gewollten Liberalisierung der Märkte, wurden diese Netze miteinander



verbunden.[17] Heute ist der Prozess Generation – Transmission – Distribution vom nationalen Netz, je nach Land zu einem unterschiedlichen Grad, entkoppelt. Der grenzüberschreitende Handel mit Strom ist erheblich höher als in der Vergangenheit. Einen Eindruck des intereuropäischen Handels gibt Abbildung 16.

**Abbildung 16: Grenzüberschreitende Energieflüsse in Europa in GWh**

Quelle: (ENTSO-E, o. J., S. 137)

Zusätzlicher Druck auf die Netze entsteht durch fortschreitende *Privatisierung* der Elektrizitätsversorgung, die laut IRGC (2006) und Kröger (2008) dazu führt, dass Unternehmen einem Preisdruck standhalten und effizient wirtschaften müssen. Dies kann ebenso den mangelnden Betrieb der notwendigen, und in der UCTE vorgeschriebenen, Redundanzen, als auch unzureichende Wartungen zur Folge haben (Kröger, 2008; IRGC, 2006). Gleichzeitig kann der wirtschaftliche Druck der

[17] Dies geschah beispielsweise durch die Richtlinie 2003/54/EC des Europäischen Parlaments und des Rates vom 26. Juni 2003 bezüglich gemeinsamer Regeln für den innereuropäischen Elektrizitätsmarkt, die die Richtlinie 96/92/EC ersetzt.



Unternehmen auch dazu führen, dass die Betreiber das Netz am Rande oder sogar über die Belastungsgrenzen hinaus operieren lassen. Diese extreme Belastung kann dazu führen, dass auch durch kleine Zwischenfälle großer Schaden entsteht (IRGC, 2006, S. 22). Ferner sind auch die Investitionen in neue Hochspannungsleitungen zurückgegangen, wodurch das Transmissions-Netz näher an seinen Kapazitätsgrenzen operiert (IRGC, 2006; Kröger, 2008). Zwar muss hier neben wirtschaftlichen Gründen auch die gesellschaftliche Inakzeptanz gegenüber neuen Leitungen als Grund genannt werden (IRGC, 2006, S, 28), jedoch kommen Gheorghe et al. (2006) zu dem Schluss, dass die Integration des europäischen Stromnetzes zu sehr unter Kostenaspekten vorangetrieben worden ist und Sicherheitsaspekte zu sehr vernachlässigt worden sind.

Die Umwandlung der Stromversorgung vom staatlichen Monopol in privatwirtschaftliche Unternehmen hat zum einen dazu geführt, dass die direkte Kontrolle des Staates eingeschränkt wurde (Bouwmans, 2006, S. 27), und zum anderen auch *keine einzelnen Besitzer oder Betreiber* mehr existieren, die für die Versorgung zuständig sind. Abbildung 17 zeigt die Organisationsstruktur des Elektrizitätssystems vor der Liberalisierung des Marktes.

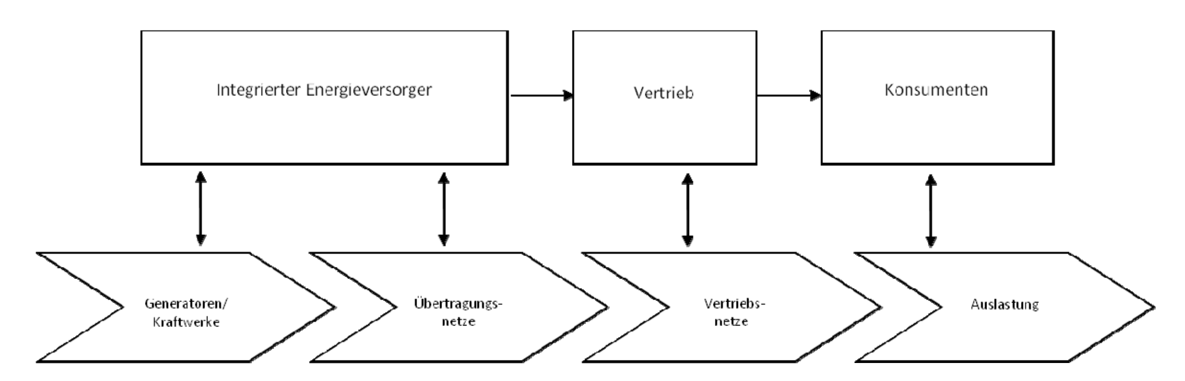



**Abbildung 17: Organisationsstruktur des Elektrizitätssystems vor der Liberalisierung**

Quelle: (eigene Darstellung in Anlehnung an Gheorge et al., 2006, S. XI)

Mit der Liberalisierung hat die Zahl der Akteure, wie in Abbildung 18 dargestellt, stark zugenommen, obwohl gleichzeitig eine Unternehmenskonzentration stattfindet; die Organisationsstruktur ist komplexer geworden. Dies macht eine aufwändigere Kommunikation notwendig und damit das System auch anfälliger, wobei transnationale Schnittstellen im Netz besondere Schwachstellen sind (IRGC, 2006). Die unzureichende Koordination von E.ON mit anderen Betreibern nach dem Stromausfall am 04. November 2006 war einer der beiden Hauptgründe für die weitreichende Störung (UCTE, 2007, S. 51).



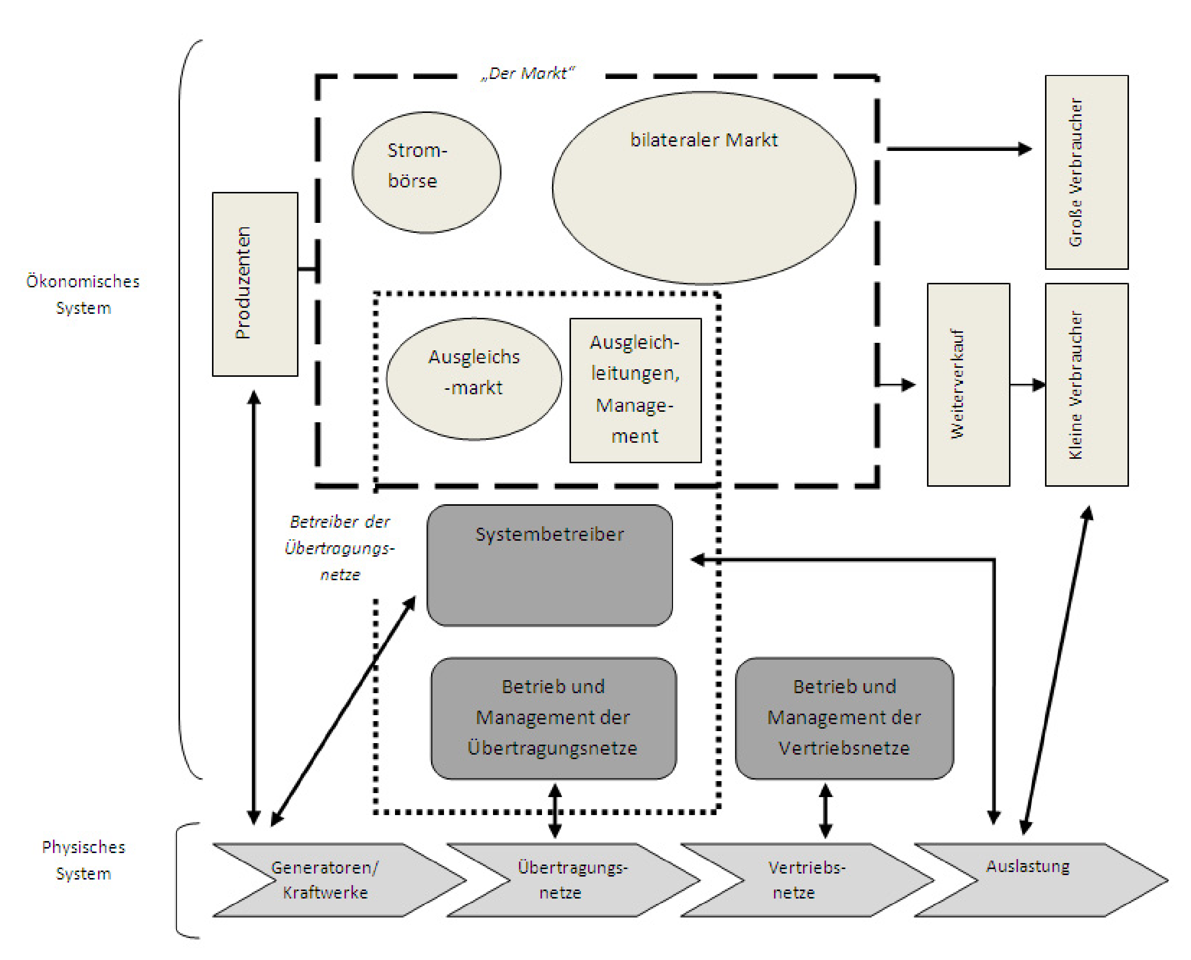



**Abbildung 18: Organisationsstruktur eines liberalisierten Elektrizitätssystems (dezentralisiertes Modell)**

Quelle: (eigene Darstellung in Anlehnung an Gheorge et al., 2006, S. VII)

## Gesellschaftliche Faktoren

Aus gesellschaftlichen Faktoren ergeben sich insbesondere Variationen im Strombedarf. Beispielsweise wachsen viele Städte, womit auch der Energieverbrauch steigt (IRGC, 2010, S. 17). Auch stellt der demographische Wandel, der die Bevölkerungsdichte in vielen Regionen Deutschlands verändert, neue Anforderungen an die Infrastruktur-systeme (Lauwe & Riegel, 2008, S. 118). Ferner ergeben sich Variationen im Strombedarf, die je nach Jahres- und Tageszeit unterschiedlich ausfallen. Zudem haben bestimmte Naturereignisse besondere Folgen für die Stromnachfrage, wie dies beispielsweise im Kontext der Hitzewellen zu verzeichnen ist (siehe Kapitel 4.1.1). Des Weiteren haben beispielsweise die Außentemperaturen einen starken Einfluss auf den Stromverbrauch. Der jährliche Strombedarf kann im UCTE-Bereich zwischen Jahren mit milden und Jahren mit kalten Wintern um ein Dutzend Terawattstunden (ThW) variieren (UCTE, 2008, S. 13).



Ferner wird der gesamte Strombedarf weiter ansteigen. Die UCTE rechnet für Deutschland mit einem jährlichen Wachstum von etwa 0,6% des Strombedarfs (UCTE, 2008, S. 16). Diese Prognose ist insofern bedenklich, als dass die Netze heute schon an ihren Grenzen operieren und neue Investitionen nur langsam getätigt werden (s.o.).

**Systembezogene Faktoren**

Die zunehmende *Komplexität* und Vernetztheit der Systeme selbst ist ein weiterer Faktor, der ihre Anfälligkeit erhöht. So nimmt nicht nur die Anzahl der Komponenten zu. Vielmehr werden die Systeme auch dadurch komplexer, dass verschiedene technologische Systeme miteinander funktionieren müssen, deren Zusammenwirken im Vorhinein nicht immer absehbar ist. Dies spielt insbesondere dann eine Rolle, wenn das System mit weitreichenden und radikalen Veränderungen konfrontiert wird (Hellström, 2007). Jedoch stellt die enorme Komplexität der Systeme auch ohne die Einführung neuer Technologien eine wichtige Komponente in der Anfälligkeit der Kritischen Elektrizitätsversorgung dar. Diese besteht insbesondere in der Vielzahl von *Abhängig-keiten* innerhalb des Systems, die dazu führen, dass der Ausfall einer Komponente den Ausfall weiterer Komponenten bedingen kann, wodurch dann Domino- oder Kaskaden-effekte entstehen können. Solche Effekte können beispielsweise dadurch ausgelöst werden, dass die Komponenten physisch oder funktional voneinander abhängig sind (Hellström, 2007, S. 426). Eine Reihe weiterer Faktoren, die die Komplexität beein-flussen, sind in Kapitel 5.3 (Erfassung der Komplexität) ausführlich erläutert.

Ein weiterer Faktor, der die Anfälligkeit beeinflusst, ist die *Abhängigkeit der Elektrizitätsversorgung von Inputs*. Dazu können im Falle der Stromversorgung sowohl IT-Inputs zur Steuerung des Netzes, als auch der Input von Verkehrsinfrastruktur zur Lieferung von Ressourcen, wie beispielsweise Kohle zum Betrieb von Kraftwerken gehören (Lenz, 2009, S. 53). Ferner ist die herkömmliche Stromversorgung immer auch auf natürliche Ressourcen wie Kohle, Uran, Gas und Öl angewiesen und so stark von Importen abhängig (BMWi und BMU, 2006, S. 11).

Im Rahmen der systembezogenen Faktoren kann ferner die *Abhängigkeit von spezifischen Umweltbedingungen* genannt werden. So sind beispielsweise Kraftwerke auf die Verfügbarkeit von Kühlwasser angewiesen. Sollte es durch extreme Trockenheit zu Wassermangel oder durch hohe Wassertemperaturen in Oberflächengewässern zu einem Engpass im Bereich des Kühlwassers oder der sog. Kühlwassereinleitung kommen, so muss der Betrieb der Kraftwerke heruntergefahren oder sogar in einigen Fällen eingestellt werden (Lenz, 2009, S. 55).



**Technologische Faktoren**

Grundsätzlich entscheidend für die Anfälligkeit der Kritischen Infrastrukturen ist ihr *Qualitätsniveau*. Da sie im Laufe der Zeit Abnutzungs- und Alterungsprozessen unterliegen, müssen sie kontinuierlich gewartet, gepflegt und erneuert werden. Dies schließt auch Maßnahmen zum *Schutz* der Komponenten gegenüber bestimmten Gefahren ein. Fehlen Wartung und Schutz, so ist die Komponente und damit der Prozess vulnerabler (Lenz, 2009, S. 56 f). Häufig ist jedoch nicht nur die Qualität der Komponente gefährdet, sondern bilden auch Schnittstellen mit dem Internet Einfallspunkte für Cyberattacken (siehe 0) (Amin, 2000, S. 268). Besonders problematisch ist in diesem Zusammenhang die Verwendung von standardisierten (off-the-shelf) Technologien. Kommerzielle Systeme haben häufig keinen, der Kritikalität der Infrastruktur angemessenen Sicherheitsstandard. Dennoch werden Produkte mit unzureichenden Sicherheitsstandards eingesetzt, was zumeist an ihrer kurzfristigen ökonomischen Effizienz liegt (Kröger, 2008, S. 1781).

Sollte eine Komponente ausfallen, so gilt als wichtigste technische Möglichkeit zur Reduktion der Anfälligkeit von KRITIS das *(n-1)-Kriterium*[18], das heute in der UCTE verbindlich ist. Jedoch ist fraglich, ob dieses Kriterium, bei dem andere Komponenten die Kapazität des ausfallenden Elementes übernehmen sollen, hinreichend umgesetzt und überwacht wird, und zudem, ob diese Maßnahme überhaupt noch den Anforderungen entspricht (IRGC, 2006, S.25). Im Falle des Stromausfalles am 04. November 2006 beispielsweise konnte das (n-1)-Kriterium im E.ON Netz nicht erfüllt werden, sodass die relativ kleine Spannungsschwankung (wie sie in einem hoch vermaschten Netz üblich ist) zum Kaskadeneffekt führte (UCTE, 2007, S. 48) und somit einer der Hauptgründe für den weitreichenden Stromausfall war. Automatisierte Systeme zum Management des Stromausfalls funktionierten nur unzureichend (Kröger, 2008).

Die *mangelnde Speichermöglichkeit für Strom* ist ein weiterer Punkt, der die Stromversorgung anfällig macht. Der Strom muss stets in dem Moment produziert werden, in dem er benötigt wird und kann nicht auf Vorrat produziert werden (BfG, 2006, S. 183 f). Zwar gibt es Speichertechnologien, wie beispielsweise Pumpspeicher-werke. Jedoch beträgt ihr Anteil zur Lastendeckung in Deutschland nur 5%; ihre Errichtung ist aus geologischen Gründen begrenzt (VDE, 2008, S. 74).

Eine weitere Herausforderung im Bereich der technologischen Faktoren sind *neue Entwicklungen*, die sich häufig in einem sehr hohen Tempo vollziehen. Dies führt zu einer Ko-Existenz von alten und neuen Bauteilen und Prozessen. Insbesondere an Schnittstellen besteht dadurch eine erhöhte Anfälligkeit des Systems (Lauwe & Riegel,

[18] Das (n-1)-Kriterium ist in Kapitel 2 näher erläutert.



2008, S. 120). In diesem Zusammenhang stellen auch erneuerbare Energien eine Herausforderung an die Netze, die ihre Nutzungsart zwangsläufig verändern müssen (Gheorge et al. 2006, S. XV).

Die Trägheit der konventionellen Kraftwerke passt derzeit nicht mit der *Dynamik der erneuerbaren Energien* zusammen, und ist damit ein letzter Punkt, der die technische Anfälligkeit der Versogung beeinflusst. Im Zuge des Ausfalls im Emsland 2006 schalteten sich beispielsweise Windkraftanlagen zu früh ins Netz hinzu. Gleichzeitig konnten die konventionellen Kraftwerke nicht schnell genug heruntergedrosselt werden, sodass die Stabilisierung der Netzgebiete erschwert wurde (Bundesnetzagentur, 2007, S. 28).

**Menschliche Faktoren**

Der Betrieb Kritischer Infrastrukturen bedarf in der Regel des Einsatzes von Fachpersonal, beispielsweise in Leitstellen. Ein möglicher Ausfall dieses Personals, beispielsweise durch Pandemien, macht die KRITIS grundsätzlich anfällig. Jedoch ist die Reduzierung der Abhängigkeit von Personal nur bedingt möglich (Lenz, 2009, S. 55). Neben einem Ausfall des Personals, der auch nur bedingt verhindert werden kann, ist menschliches Versagen ein weiterer Faktor, der die Anfälligkeit des Elektrizitäts-sytems mit beeinflusst. Hierbei können drei verschiedene Fehlertypen identifiziert werden (Reason, 1994, S. 81):

- *„Fähigkeitsbasierte Patzer"*
- *„Regelbasierte Fehler"*
- *„Wissensbasierte Fehler"*

Während *fähigkeitsbasierte Patzer* menschliche Fehler bei der Umsetzung von Handlungen sind, handelt es sich bei *Fehlern* um Vorgänge, die nach Plan ablaufen könnten, bei denen aber der Plan nicht ausreicht, um das gewünschte Resultat zu erzielen (Reason, 1994, S. 81). Im Rahmen der Elektrizitätsversorgung sind entsprechend dieser Kategorien drei Probleme zu nennen:

1. *Fähigkeitsbasierte Patzer* können sowohl durch Unaufmerksamkeit als auch durch Überaufmerksamkeit (wenn beispielsweise die aktuelle Situation als weiter fortgeschritten eingeschätzt wird, als sie tatsächlich ist) entstehen.
2. *Regelbasierte Fehler* können u.a. in Folge unzureichender Notfallpläne auftreten. Insbesondere ein Defizit an Koordination und bindender Regeln zwischen den europäischen Betreibern für den Umgang mit Notfallsituationen werden in diesem Zusammenhang erwähnt (IRGC, 2006, S. 28).
3. Der Mangel von Echtzeitinformationen stellt im Umgang mit Schwankungen im Netz und Störungen ein Defizit dar, das zu *wissensbasierten Fehlern* führen kann (IRGC, 2006, S. 28). Im Zusammenhang mit dem Auftreten dieser Art von



> Fehlern muss zudem in der Komplexität des Elektrizitätssystems selbst gesehen werden (siehe hierzu auch Kapitel 5.3), die es dem Bediener immer schwieriger macht, die richtigen Entscheidungen zu treffen (Reason, 1994, S. 216 ff).

Während des Stromausfalls im Emsland am 4. November 2006 traten einige der oben genannten *Fehler* auf (siehe hierzu auch Kapitel 4.1.3). So hatte beispielsweise der Betreiber E.ON die anderen betroffenen Betreiber erst kurz vorher über die verfrühte Abschaltung der Leitung informiert. Auch war nach der Aufsplittung des Gesamtnetzes die Gesamtlage für die Betreiber zunächst unübersichtlich (UCTE, 2007, S. 55 f). Ein klares Bild der Situation des Ausfalls (basierend auf Echtzeit-Daten) stand nicht zu jedem Zeitpunkt zur Verfügung und die Vorbereitung auf einen Notfall war nicht ausreichend (Kröger, 2008; IRGC, 2006, S.22).

**Zwischenfazit Anfälligkeit**

Zusammenfassend lässt sich feststellen, dass es fünf Kernbereiche gibt, die die Anfälligkeit von Kritischer Elektrizitätsversogung negativ beeinflussen können. Hierzu gehören zunächst *Institutionelle Faktoren*. In diesem Bereich stellt insbesondere die Liberalisierung des Marktes und die damit einhergehende Nutzung der Netze für den internationalen Stromtransfer, für den diese nicht geschaffen worden sind, einen Einflussfaktor auf die Anfälligkeit der Elektrizitätsversorgung dar. Auch ist die Anzahl der Akteure auf dem Markt, die ihre Arbeit koordinieren müssen stark gewachsen, was die Anfälligkeit erhöht. Ferner wirkt sich auch die Privatisierung und damit möglicher Preisdruck negativ auf die Verwundbarkeit des Systems auswirken, so dass in diesem Bereich Lösungsansätze gefunden werden müssen.

Neben den systemischen spielen jedoch auch *gesellschaftliche Faktoren* eine Rolle, wie beispielsweise sich verändernde Nachfrage und Bevölkerungsdichte. Ferner wirken *systembezogene Faktoren* wie die Komplexität der Elektrizitätsversorgung selbst und ihre Abhängigkeit von anderen Infrastrukturdienstleistungen, wie beispielsweise IT-Services, auf die Verwundbarkeit. Sie machen das Gesamtsystem schwerer berechen- und steuerbar.

Im Rahmen der *technologische Faktoren* ist fraglich, ob notwendige Wartung, Pflege und Erneuerung auch unter Kostendruck den Anforderungen entsprechend durchgeführt werden. Insbesondere muss überprüft werden, ob der hauptsächlich verwendete (n-1)-Sicherheitsstandard noch den Anforderungen entspricht. Die Integration neuer Technologien sowie die mangelnde Speichermöglichkeit für Strom stellen weitere Herausforderungen dar.

Schließlich wirken auch *menschliche Faktoren* auf die Elektrizitätsversorgung ein, die auf Fachpersonal angewiesen ist, das Kontrollfunktionen, beispielsweise in Leitstellen übernimmt. Hier kann es jedoch zu Fehlern kommen, wenn verbindliche Regeln und



internationale Absprachen zum Umgang mit Notfallsituationen fehlen. Auch der mangelnde Überblick über die Sachlagen aufgrund fehlender Echtzeit-Daten ist kritisch zu bewerten.

## 4.3 Bewältigungskapazität

f (Vulnerabilität) = Exposition (Gefahr), Anfälligkeit, **Bewältigungskapazität**

Wie im Kapitel 3.2 erläutert, steht Bewältigungskapazität für das Anwenden der vorhandenen Möglichkeiten, um Umständen entgegenzutreten, die zu einer Krise oder Katastrophe führen könnten (UN/ISDR, 2004, S. 2), und beschreibt damit, im Gegensatz zur Anfälligkeit, Faktoren, die die Verwundbarkeit reduzieren können. Insbesondere in Bezug auf Kritische Infrastrukturen hat Lenz (2009) eine Definition entwickelt, bei der unter Bewältigungskapazität jegliche Maßnahmen und Ressourcen gefasst werden, „die vor, während und nach Eintritt eines Ereignisses ergriffen werden können, um negative Auswirkungen zu begrenzen und den Normalzustand wiederherzustellen“ (Lenz, 2009, S. 41). Bewältigungskapazität ist folglich ein dynamischer Prozess.

Um die Bewältigungskapazität zu bestimmen und somit für den Gegenstand KRITIS greifbar zu machen, gibt es unterschiedliche Indikatoren. Diese stellen sich unter anderem in Bereitschaft, Umfeld, Redundanz, Transparenz, Wiederherstellungsaufwand sowie Dezentralisierung dar (siehe Abbildung 19) (Lenz, 2009, S. 58 ff).

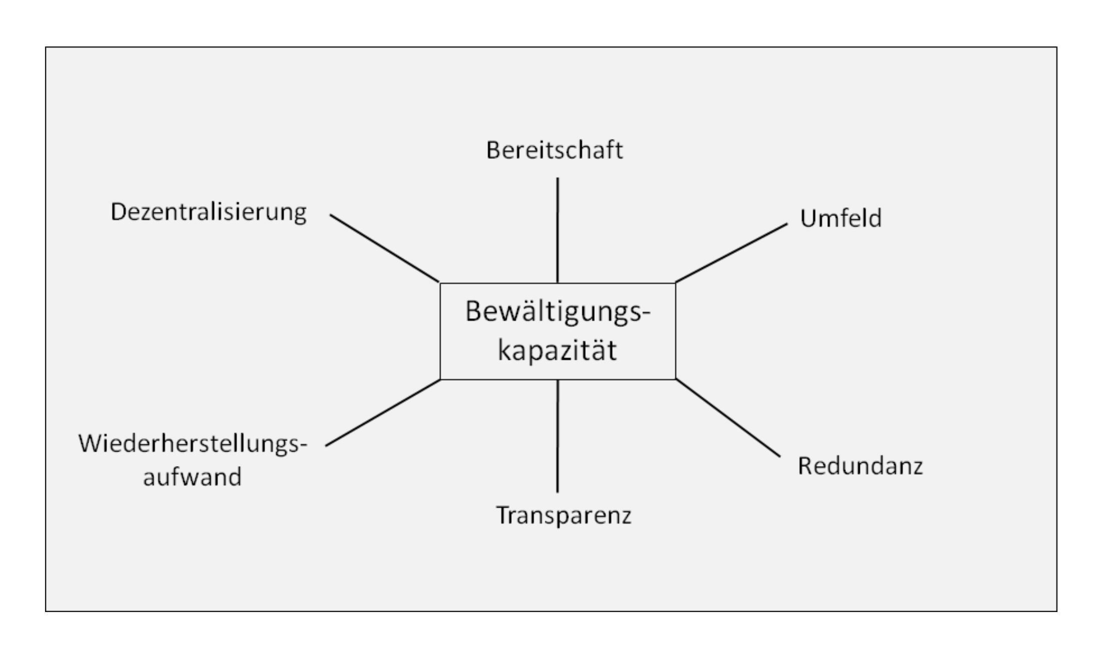



**Abbildung 19: Indikatoren der Bewältigungskapazität**

Quelle: (eigene Darstellung)



Unter **Bereitschaft** wird dabei verstanden, dass die Bewältigung durch ausreichende Vorbereitungen leichter durchzuführen ist, wodurch eine Störung schneller behoben werden kann. Somit wird die Bereitschaft als *„relatives Maß für den Grad, in dem Vorbereitungen für den Umgang mit und die Bewältigung von Störungen bzw. Schäden im Hinblick auf die Aufrechterhaltung bzw. schnelle Wiederherstellung der Funktionsfähigkeit einer KRITIS getroffen sind"* definiert (Lenz, 2009, S. 58). Im Umkehrschluss bedeutet dies, dass eine Erhöhung der Bereitschaft die Bewältigungskapazität stärkt. Als praktisches Beispiel ist dabei exemplarisch die Schulung von Personal, die Erstellung von Krisen- und Notfallplänen, die Durchführung von vorbereitenden Notfallübungen (siehe dazu auch Kapitel 6.3) wie auch schließlich die Ausarbeitung funktionierender Back-up-Systeme[19] zu sehen (Lenz, 2009, S. 58; Schäuble, 2010).

Neben der Bereitschaft ist auch das **Umfeld** eine Einflussgröße der Bewältigungskapazität. Darunter wird unter anderem die politische Stabilität eines Staates verstanden. Ist ein Staat in seinen Strukturen und seiner Staatsform stabil, so ist es für diesen in der Regel einfacher, eine Krisensituation aus eigener Kraft zu bewältigen, als wenn instabile Strukturen vorherrschen (Meyer, K., o.J.). Auch ist das Verhältnis zwischen privaten Unternehmen und dem öffentlichen bzw. staatlichen Interesse als ein wichtiger Faktor anzusehen, denn die Interessen dieser beiden Parteien können im Bereich KRITIS stark divergieren. So besteht beispielsweise durch den Preisdruck bei privaten Unternehmen die Gefahr, dass bei der Einrichtung von Redundanzen sowie bei der Wartung von Netzen Gelder eingespart werden, und es dadurch zu Sicherheitsrisiken kommt. Daraus können Interessenskonflikte zwischen privaten Unternehmen und dem öffentlichen und staatlichen Interesse resultieren. Während die privaten Unternehmen vor allem die Wirtschaftlichkeit ihres Unternehmens verfolgen, stellt für die Öffentlichkeit und den Staat Sicherheit ein unverzichtbares Gut dar. Daher muss solchen Divergenzen entgegengewirkt werden, um die Anfälligkeit zu verringern beziehungsweise die Bewältigungskapazität zu erhöhen (IRGC, 2006; Kröger, 2008; Fritzon et al., 2007, S. 37 f).

**Redundanz** als weiterer Indikator für die Bewältigungskapazität beschreibt den Zustand, dass mehrfache Strukturen existieren, welche dieselbe Leistung erbringen und somit die Bewältigung einer Störung verbessern. Redundanz wird demnach als *„relatives Maß für das mehrfache Vorhandensein von Strukturen zur Erbringung derselben Leistung"* definiert (Lenz, 2009, S. 58). Dies bedeutet, dass – vorausgesetzt es sind redundante Strukturen vorhanden – die Funktionsfähigkeit eines Systems auch dann aufrechterhalten werden kann, wenn der Ausfall einzelner Komponenten vorliegt

[19] Weitere Ausführungen zu den Back-up-Systemen folgt unter dem Punkt Redundanz.



(siehe Abbildung 20). Insgesamt führt das Vorhandensein von Redundanzen zur Erhöhung der Bewältigungskapazität (Lenz, 2009, S. 58).

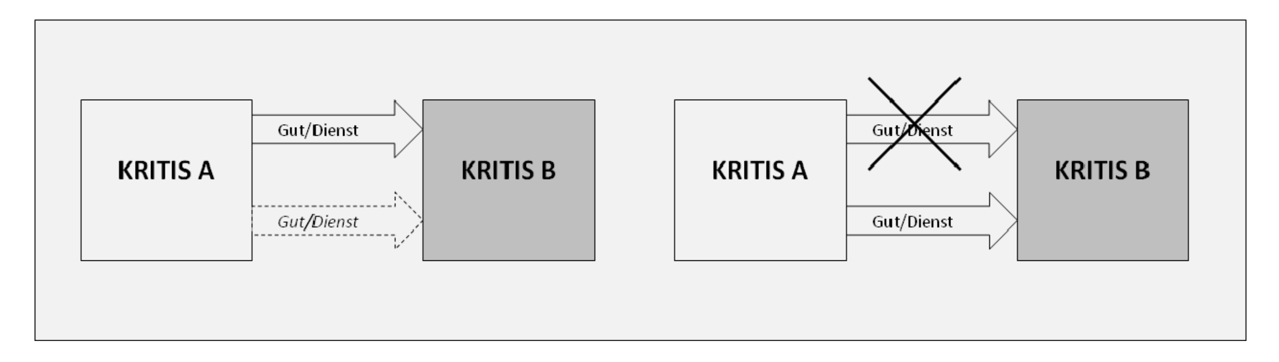



Abbildung 20: Redundanz

Quelle: (Lenz, 2009, S. 58)

Ein Beispiel für eine Redundanz sind beispielsweise die im mittleren Rheintal parallel verlaufenden Bahntrassen. Die eine Trasse befindet sich links-, die andere rechtsrheinisch. Auf der rechtsrheinischen Bahnstrecke verkehrt vor allem der Güterverkehr, auf den linksrheinischen Schienen werden Personen befördert. Fällt eine Trasse auf einer Seite aufgrund einer Störung aus, so kann auf die andere Trasse umgeleitet werden (Lenz, 2009, S. 58 f). Bei der Stromversorgung wird dieser Zusammenhang häufig als (n-1)-Kriterium beschrieben. Dennoch kann auch durch die Redundanzen keine vollkommene Versorgungssicherheit hergestellt werden. Werden beispielsweise die Strommasten durch hohe Schneelast oder starke Orkanböen abgeknickt, können auch Redundanzen, welche bei den Stromleitungen konzipiert wurden, keinen Ausfall verhindern[20] (RWE, 2006).

Sogenannte **Back-ups** stellen eine besondere Form von Redundanzen dar. Dies sind technische Vorrichtungen, welche im Notfall eingesetzt werden. Ein Beispiel für Back-ups kann in Notstromaggregaten gesehen werden. Diese können bei einem Stromausfall eingesetzt werden und den Ausfall überbrücken. Sie werden erst im Notfall eingesetzt und nicht – wie es bei anderen Strukturen der Fall ist – im alltäglichen Betrieb genutzt (Lenz, 2009, S. 58 f; McDaniels et al., 2008, S. 315). Ein Beispiel für

[20] Ein Beispiel hierfür liefert die Gemeinde namens „Ochtrup“ im nordwestlichen Münsterland. Bei dieser Gemeinde ist die Stromanbindung durch das (n-1)-Kriterium konzipiert worden, wobei der Ort auf zwei verschiedenen Wegen angebunden ist. Nach Ochtrup führen dabei jeweils von Nordwesten sowie von Südosten kommend Hochspannungsleitungen mit jeweils zwei Stromkreisläufen auf die Stadt zu. Die Stromleitungen werden kurz vor der Stadt vereint und dann in die Stadt eingeleitet. In der Nacht vom 25.11.2005 wurden allerdings durch das Zusammenspiel von hoher Schneelast, starkem Wind und Eisregen (siehe Kapitel 4.1.3) die Maste in beiden Richtungen abgeknickt und damit alle vier Anbindungsmöglichkeiten zerstört. Trotz vorhandener Redundanzen war die Stromversorgung der Gemeinde Ochtrup somit unterbrochen (RWE, 2006).



einen eingesetzten Back-up ist in den Notstromaggregaten des Rechenzentrums einer Firma in Karlsruhe zu sehen. Die Notstromaggregate kamen dort am 30. Januar 2008 bei einem Stromausfall zum Einsatz. Der Stromausfall wurde durch einen Brand in einem Umspannwerk am Rheinhafen ausgelöst. Daraufhin war ab 17:35 Uhr im Westen und Osten der Stadt ein kompletter Stromausfall zu verzeichnen. Die umfassende Stromversorgung war erst wieder ab ca. 19 Uhr gewährleistet. Das Rechenzentrum hat für Stromausfälle einen Notfallplan, der bei diesem Blackout griff. Dabei kam es zu einer Abtrennung vom öffentlichen Stromnetz nachdem eine Unterschreitung der Netzspannung stattgefunden hatte. Für die ersten Minuten des Stromausfalls sprangen riesige Akkus ein, mit denen die unterbrechungsfreie Stromversorgung erst einmal gewährleitet werden konnte. Gleichzeitig liefen vier Dieselmotoren (Notstromaggregate) an. Durch das Anspringen der Aggregate wurden die Akkus nachgeladen und die Stromversorgung konnte somit sichergestellt werden. Zudem existieren als Reserve ein zusätzlicher Batterieblock sowie ein redundanter Dieselmotor, um die Stromversorgung zu gewährleisten (Dederichs, 2010).

Unter dem weiteren Indikator **Transparenz** versteht Lenz das relative *„Maß für die Nachvollziehbarkeit der Zusammensetzung und Funktionsweise einer Kritischen Infrastruktur“* (Lenz, 2009, S. 60). Dabei lässt sich eine generelle Zunahme der Komplexität Kritischer Infrastrukturen feststellen, wodurch eine Transparenz erschwert und damit der Bewältigungskapazität entgegengewirkt wird (Lenz, 2009, S. 60). Neben dieser eher technischen Sichtweise, welche die Kritische Infrastruktur selbst betrifft kann unter Transparenz aber auch der Informationszugang bzw. die Kommunikation unter den einzelnen Akteuren gefasst werden. Im Falle einer Störung des Elektrizitätsnetzes kommt dieser Risiko- und Krisenkommunikation eine herausragende Stellung zu. Die Kommunikation wird durch Reichenbach et al. (2008) dabei in vier Ebenen unterteilt:

- Die <u>erste Ebene</u> beschreibt die Kommunikation im Vorfeld und kann damit als Präventivmaßnahme beschrieben werden.
- Die <u>zweite Ebene</u> beschreibt die Kommunikation im Krisenfall selbst und ist damit reaktiv.
- Die <u>dritte Ebene</u> stellt die Kommunikation nach innen, also zwischen den Akteuren der Gefahrenabwehr dar, während
- die <u>vierte Ebene</u> die Kommunikation nach außen, mit der Bevölkerung betrifft.

Eine entscheidende Rolle spielen in der Krisenkommunikation die Medien. Durch diese kann eine Verstärkung, aber auch eine Abschwächung einer Krise stattfinden. So kann beispielsweise im Falle unzureichender oder ausbleibender Verständigung eine Krise verschärft werden (Reichenbach, et al., 2008, S. 26).



Weiter wird die Bewältigungskapazität verbessert, wenn der **Wiederherstellungsaufwand** nach einer Störung oder Beschädigung einer Kritischen Infrastruktur schnell und wirtschaftlich vonstattengeht. Somit wird der Wiederherstellungsaufwand als *„relatives Maß für den zeitlichen und finanziellen Aufwand, der mit einer Wiederherstellung der KRITIS und ihrer Funktionsfähigkeit nach Beschädigung oder Zerstörung verbunden wäre“* definiert (Lenz, 2009, S. 60). Daher ist schon im Voraus, vor eventuellen Schäden an Kritischen Infrastrukturen, zu planen, wie diese am besten konzipiert werden können, um den Wiederherstellungsaufwand möglichst gering und wirtschaftlich zu halten (Lenz, 2009, S. 60).

Schließlich soll an dieser Stelle diskutiert werden, ob die **Dezentralisierung** des Stromnetzes als ein Indikator für die Bewältigungskapazität angesehen werden kann. Während sich das herkömmliche Stromnetz noch durch eine zentralisierte Stromerzeugung auszeichnet, die zu einem Großteil aus Großkraftwerken gespeist wird, soll neben dem Klimaschutz durch die Einführung erneuerbarer Energien mit vielen verteilten Anlagen eine Dezentralisierung der Stromerzeugung erzielt werden. Diese kann unter anderem Windanlagen, Kraft-Wärme-Kopplungen, Biomasse- und Biogasanlagen sowie Fotovoltaik-Anlagen umfassen[21] (siehe dazu Abbildung 21). Das vorrangige Ziel der Einführung der erneuerbaren Energien besteht darin, dem hohen Verbrauch fossiler Brennstoffe sowie dem Bestand von Atomkraftwerken entgegenzuwirken (Haas & Redl, 2009, S. 63; Oberweis, 2006, S. 27).

Ein Punkt, der für die Dezentralisierung als Indikator der Bewältigungskapazität sprechen könnte, ist in der Erhöhung der Versorgungssicherheit zu sehen. Diese kann vor allem dadurch erreicht werden, dass durch die erneuerbaren Energiegewinnungsanlagen die Rohstoffabhängigkeit fossiler Brennstoffe sinkt. Auch wird Stromimporten aus dem Ausland entgegengewirkt, da durch die kleineren dezentralen Einspeiseeinheiten insbesondere eine höhere Verfügbarkeit erzielt wird. Dies hat den weiteren Vorteil, dass diese nahe beim Verbraucherschwerpunkt aufgebaut werden können. In diesem Zusammenhang wird auch Transportverlusten entgegengewirkt (Oberweis, 2006, S. 27 f).

Ein weiterer Punkt, der für die Dezentralisierung als Indikator für die Bewältigungskapazität spricht, ist darin zu sehen, dass durch die Einführung erneuerbarer Energien ein Innovationsschub ausgelöst wird und neue Technologien entwickelt werden, um die Versorgung aus vielen dezentralisierten Energiequellen zu koordinieren. Dadurch kann

[21] Die Unterscheidung herkömmlicher Energiegewinnung von erneuerbaren Energien besteht auch hinsichtlich der Leistungsklassen sowie den entsprechenden Einspeiseebenen in das elektrische Netz. Die Obergrenze des Leistungsspektrums bilden herkömmliche Großkraftwerke, welche sich in verschiedene Stromerzeugungsverfahren unterteilen lassen und die Energie in das Hochspannungsnetz einspeisen. Dezentrale Erzeugungsenergien speisen demgegenüber die Energie in das Verteilungsnetz (Mittelspannungsebene) ein (Haas & Redl, 2009, S. 63).



ein gezieltes Lastmanagement der Energieerzeugung und dem Verbraucherverhalten stattfinden. Wenn es zukünftig gelingt, ein solches sogenanntes „intelligentes Stromnetz“ aufzubauen kann dies zu einer weiteren Erhöhung der Versorgungssicherheit beitragen und damit auch die Bewältigungskapazität erhöhen (siehe dazu auch ausführlicher Kapitel 6.3.3 erneuerbare Energien) (Oberweis, 2006, S. 27 f; Haber & Bliem, 2010, S. 3).

Dennoch muss auch festgestellt werden, dass die hier aufgezeigten Entwicklungen erst einmal auf dem Markt etabliert werden müssen. Bisher befindet sich der Ausbau einer dezentralen Elektrizitätsversorgung am Anfang und es muss abgewartet werden, inwiefern neue Probleme durch noch nicht abzuschätzende Faktoren entstehen. So könnte es beispielsweise sein, dass sich die Komplexität von Systemen durch die vielen kleinen Energieerzeugungsanlagen weiter erhöht. Somit sind die künftigen Entwicklungen abzuwarten, um beurteilen zu können, inwieweit eine Dezentralisierung der Elektrizitätsversorgung die Bewältigungskapazität erhöhen kann.



Großkraftwerk speist über die Hochspannungsebene
in das Verteilungsnetz

Versorgungsstruktur nach dezentralem Konzept

Verbraucher:
Klein- und Mittelunternehmen
Haushalte
Gewerbe, Handel und Verkehr

PV-Anlagen

Biomassekraftwerk

Einspeisung über Trafo in die
Mittelspannungsebene

Windenergieanlagen

Kleinwasserkraftanlage

Blockheizkraftwerk

**Abbildung 21: Die dezentrale Elektrizitätsversorgung – Elemente eines vernetzten Systems**

Quelle: (Oberweis, 2006, S. 26)

### Zwischenfazit Bewältigungskapazität

Für die Bestimmung der Bewältigungskapazität können verschiedene Indikatoren herangezogen werden, welche sich unter anderem in Bereitschaft, Umfeld, Redundanz, Transparenz, Wiederherstellungsaufwand und Dezentralisierung darstellen lassen:

- *Bereitschaft:* Liegen Vorbereitungen und Übungen vor, kann besser auf Störungen einer KRITIS reagiert und diese schneller behoben werden. Die Bewältigung ist dadurch leichter durchzuführen.



- *Umfeld:* Die politische Stabilität eines Staates aber auch das Verhältnis privatisierter Unternehmen und dem öffentlichen beziehungsweise staatlichen Interesse können einen großen Einfluss auf die Bewältigungskapazität haben.
- *Redundanz:* Wenn redundante Strukturen vorliegen, existieren mehrfache Strukturen, die dieselbe Leistung erbringen. Somit kann ein System auch dann aufrecht erhalten werden, wenn einzelne Komponenten ausfallen. Eine bestimmte Form von Redundanzen stellen sogenannte Back-ups dar. Diese technischen Vorrichtungen werden nur im Notfall eingesetzt (Bsp. Notstrom-aggregat).
- *Transparenz:* Die Nachvollziehbarkeit der Funktionsweise sowie Zusammen-setzung einer KRITIS ist von entscheidender Bedeutung, um im Fall einer Störung reagieren zu können. Daneben ist aber auch die Kommunikation unter den jeweiligen Akteuren von großer Bedeutung, um dadurch den Vorfall transparenter zu gestalten und die Krise schneller zu bewältigen.
- *Wiederherstellungsaufwand:* Wenn der Wiederherstellungsaufwand nach einer Störung oder Beschädigung einer KRITIS schnell und wirtschaftlich vonstatten geht, wird die Bewältigungskapazität erhöht.
- *Dezentralisierung:* Durch die Einführung erneuerbarer Energien soll dem Verbrauch fossiler Brennstoffe sowie der Abhängigkeit von Atomenergie entgegengewirkt und der Klimaschutz gestärkt werden. Die daraus resultierende Dezentralisierung des Stromnetzes birgt die Chance, die Versorgungssicherheit weiter auszubauen, sowie Stromimporten und Transportverlusten entgegenzu-wirken. In diesem Zusammenhang neu entwickelte Technologien, wie beispielsweise Smart Grids, können zu einem weiteren Anstieg der Ver-sorgungssicherheit und Verbrauchssteuerung führen. Da die erneuerbaren Energien jedoch gerade erst ausgebaut werden und zum jetzigen Zeitpunkt noch eine zentrale Struktur der Stromversorgung vorliegt, ist abzuwarten, inwieweit dezentralisierte Stromnetze die Bewältigungskapazität zukünftig erhöhen können.



# 5 Verwundbarkeit des Systems „KRITIS-Mensch“

Da die Energieversorgung als Basisinfrastruktur die Voraussetzung für das Funktionieren anderer KRITIS ist, muss neben einer Abschätzung ihrer Vulnerabilität auch der Grad der Abhängigkeit anderer Infrastrukturen untersucht werden. Gleiches gilt für die Wechselwirkungen zwischen Bevölkerung und Elektrizitätsversorgung, um eine umfassende Einschätzung der Auswirkungen eines Ausfalles zu gewährleisten. Einige dieser Abhängigkeiten zwischen Bevölkerung und KRITIS sind in Abbildung 22 dargestellt:

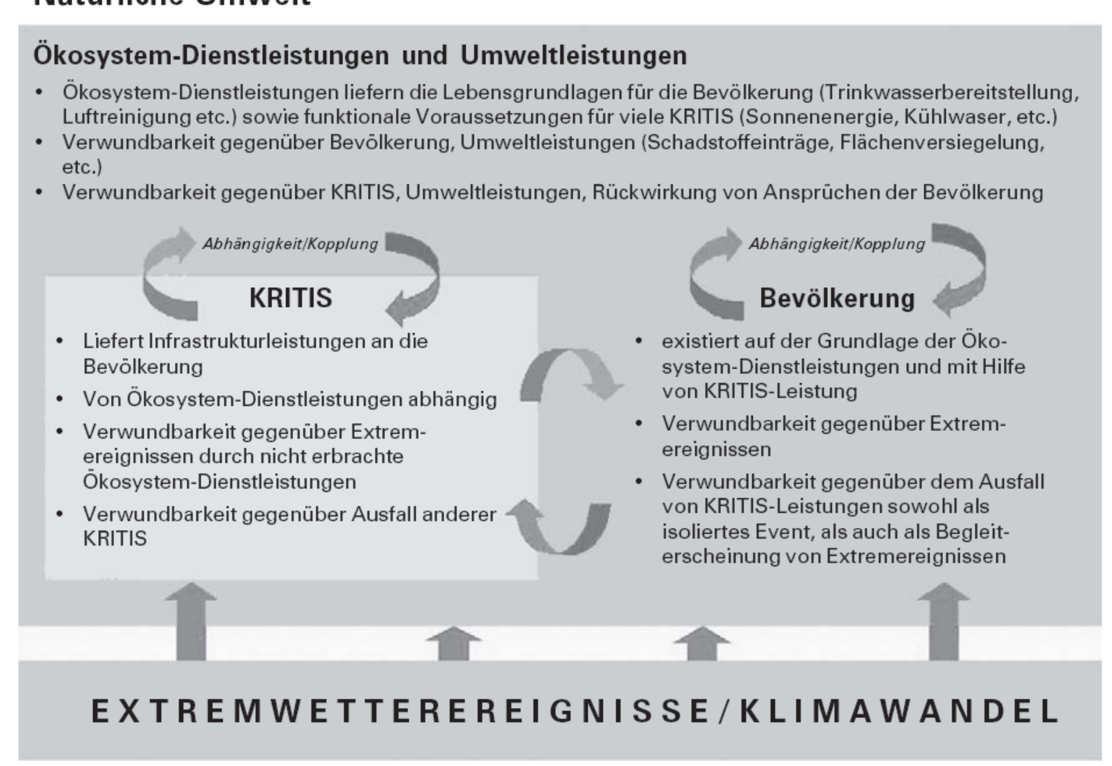



**Abbildung 22: Interaktionsschema zu Umweltbedingungen, Bevölkerung und KRITIS unter dem Einfluss des Klimawandels**

Quelle: (Birkmann & Krings, 2008, S. 4)

## 5.1 Abhängigkeit anderer KRITIS von der Elektrizitätsversorgung

Wie bereits eingangs beschrieben, besteht die besondere Brisanz von möglichen Stromausfällen in der Eigenschaft der Elektrizität, die von vielen anderen Kritischen Infrastrukturen und zur Gewährleistung zentraler Daseinsfunktionen (Wohnen, Mobilität/Verkehr, Ver- und Entsorgung) benötigt wird. Abbildung 23 zeigt, welche anderen Kritischen Infrastrukturen bei einem Stromausfall betroffen sein können:



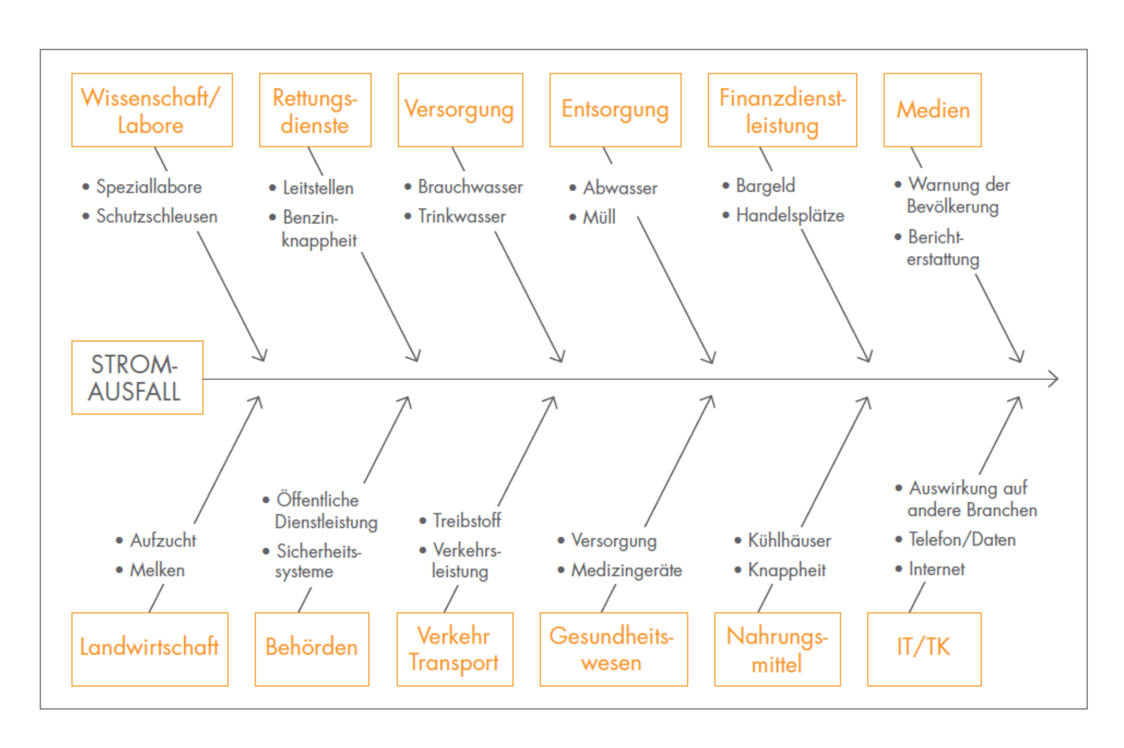



**Abbildung 23: Auswirkungen eines Stromausfalls auf andere KRITIS**

Quelle: (Reichenbach et al., 2008, S. 22)

So ist beispielsweise die Wasserversorgung vielfach direkt an die Stromversorgung geknüpft, da sowohl Pumpen, als auch Steuerungs- und Überwachungssysteme der Elektrizität bedürfen. Auch das Finanz- und Bankenwesen wäre im Falle eines langanhaltenden, flächendeckenden Stromausfalls außer Funktion, da Geld- und Kassenautomaten ebenso wenig funktionieren würden wie der elektronische Zahlungsverkehr oder der Wertpapierhandel (Reichenbach et al., 2008, S. 22).

Dabei ist zu beachten, dass diese Abhängigkeiten nicht nur direkt, sondern auch indirekt bestehen können. Einige Beispiele zeigt Abbildung 24. So können durch den Ausfall des Stroms Öl-Pipelines betroffen sein (First-Order Effects), was wiederum zur Verknappung des Öls (Second-Order Effects) und damit zu Störungen des Straßen- und Flugverkehrs (Third-Order Effects) führen könnte. Ferner haben beispielsweise die Auswirkungen eines Stromausfalls und die damit verknüpften Ketteneffekte an sogenannten *neuralgischen Knotenpunkten* der Verkehrsinfrastruktur direkte ökonomische Folgen. So fertigt der Flughafen Düsseldorf International jährlich 18 Millionen Passagiere und 97.000 Tonnen Luftfracht ab; im Hamburger Hafen werden im gleichen Zeitraum sogar 10 Millionen Container umgeschlagen, die bei einem Stromausfall, zumindest kurz- bis mittelfristig nicht an ihren Zielort gebracht werden können (Küchle, 2009, S. 15 f).



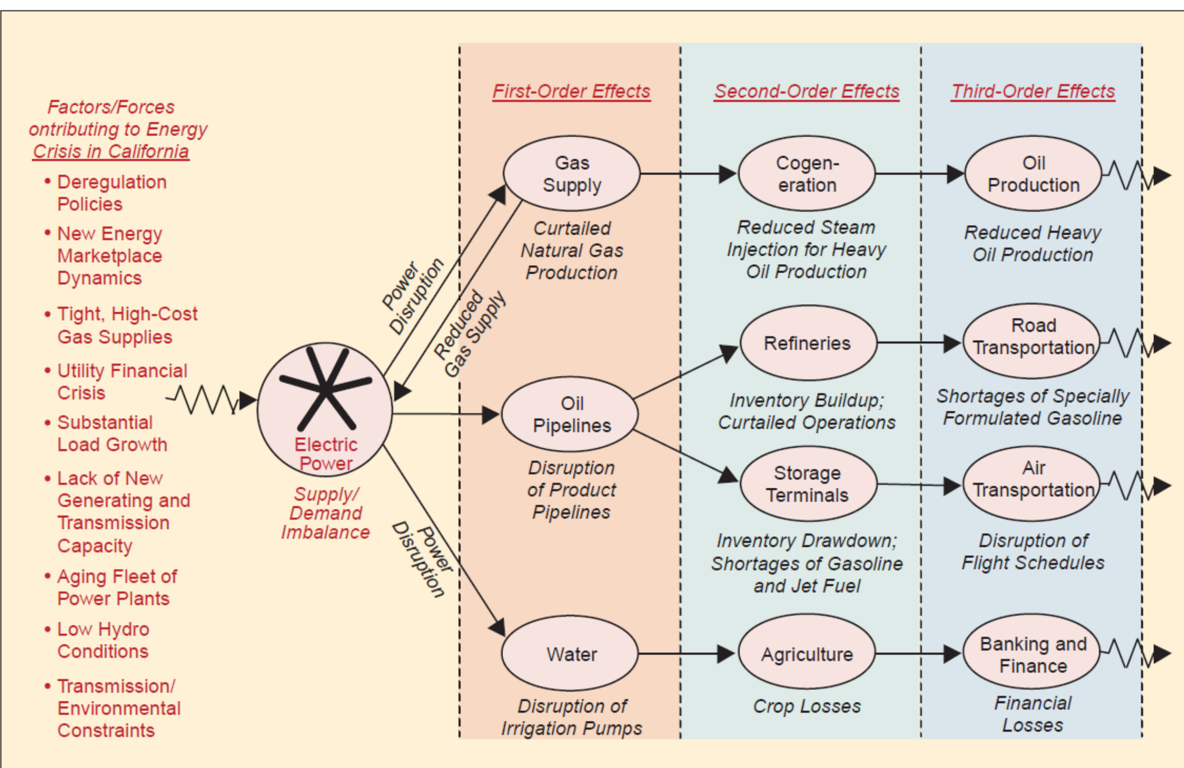



**Abbildung 24: Mögliche Auswirkungen eines Stromausfalls**

Quelle: (Rinaldi et al., 2001, S. 19)

Da die Abhängigkeiten anderer Infrastrukturen von der Stromversorgung vielfältig und wirtschaftlich bedeutend sind, kann die Reduzierung ihrer Vulnerabilität einen wichtigen Beitrag zur öffentlichen Sicherheit leisten. Auch umfassende Kenntnisse zu Kopplung verschiedener Sektoren und den Arten ihrer Verknüpfung ist wichtiges Wissen, um die möglichen Auswirkungen eines Stromausfalls umfassend zu verstehen und geeignete Schutzmaßnahmen ergreifen zu können. Dies ist jedoch aufgrund der Komplexität der einzelnen Sektoren und ihrer zahlreichen Interdependenzen und Verknüpfungen sehr umfangreich und bisher kaum geschehen (siehe hierzu auch Kapitel 5.3). Forschung kann zudem auch dadurch behindert werden, dass viele Informationen von Unternehmen vertraulich behandelt werden und der Wissenschaft so kaum zugänglich sind.

## 5.2 Abhängigkeit der Bevölkerung von Kritischer Elektrizitäts-infrastruktur

Im Falle eines langanhaltenden Stromausfalls ist die Bevölkerung direkt und in allen Lebensbereichen betroffen. Dabei werden neben Heizung bzw. Kühlung das elektrische Licht sowie Telefon, Internet und Rundfunk-/ TV-Empfang ausfallen (siehe Abbildung 25). Auch Probleme in der Versorgung mit Lebensmitteln sind zu erwarten, da die Trinkwasserversorgung und der Betrieb von Kühl- und Gefrierschränken zur Lebens-mittelbevorratung ausfallen können. Ferner kann auch die Entsorgung des Abwassers



durch längeren Stromausfall beeinträchtigt werden, mit der Folge entsprechender Gesundheitsrisiken (Reichenbach et al., 2008).

Durch die Abhängigkeit anderer KRITIS von der Stromversorgung (siehe auch Kapitel 5.1) ist die Bevölkerung auch indirekt durch den Ausfall diverser Dienste betroffen. Hierzu gehören beispielsweise der Öffentliche Personennahverkehr (ÖPNV), als auch der Individualverkehr in Städten, der durch den Ausfall von Ampeln und Straßen-beleuchtung nicht oder nur eingeschränkt aufrecht erhalten werden kann. Auch der Einzelhandel müsste schließen, da weder Kassensysteme noch Kühlung oder Licht funktionieren. Ein weiteres Problem besteht in dem möglichen Ausfall der Notdienste, die zwar häufig durch Notstromaggregate einen kurzfristigen Stromausfall überbrücken können, bei längerfristigen Störungen jedoch auch betroffen sein können (Reichenbach et al., 2008).

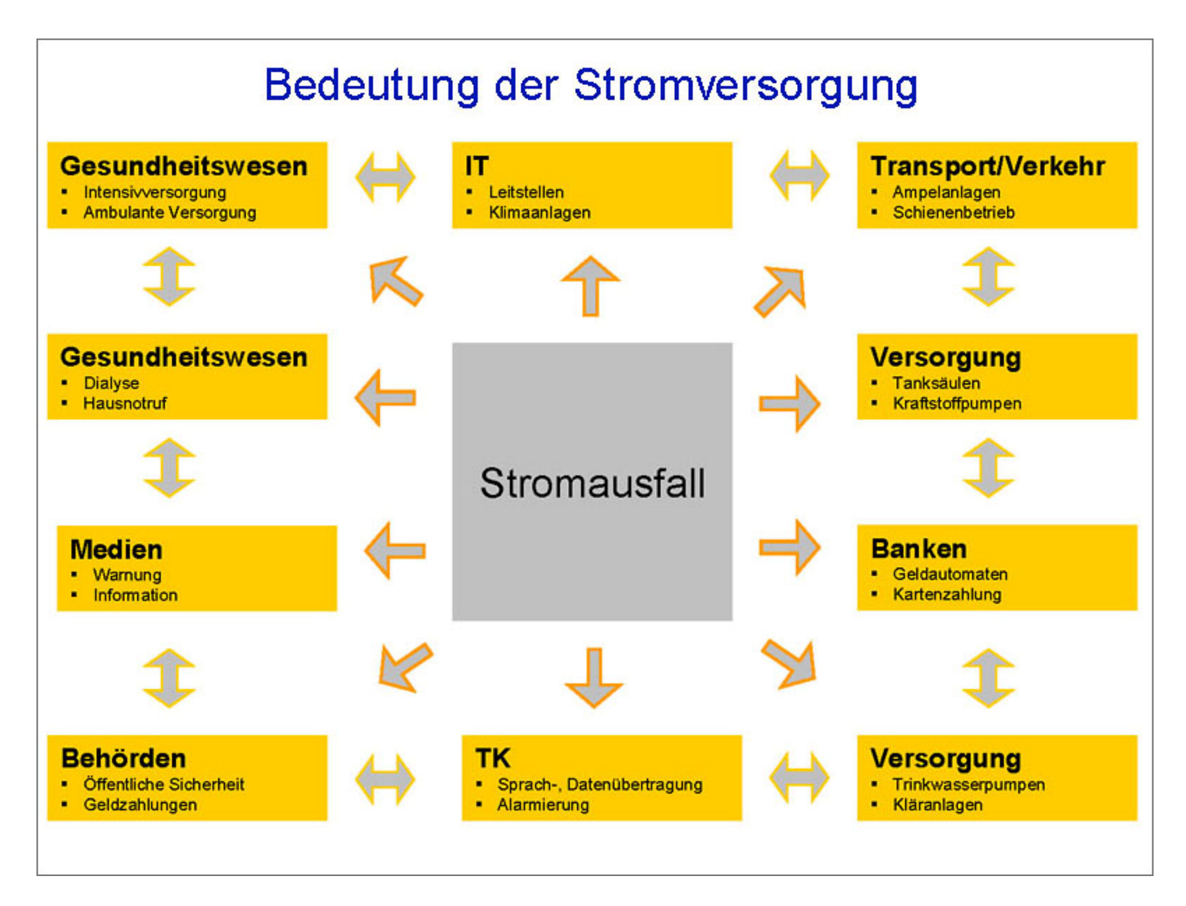



**Abbildung 25: Bedeutung der Stromversorgung**

Quelle: (BBK, 2010a)

Letztendlich sind die Auswirkungen eines Stromausfalls auf die Bevölkerung von vielen Faktoren abhängig. So beispielsweise von der Art der betroffenen Region, der Dauer des Ausfalls und der Tageszeit, zu der er passiert (Holmgren, 2007). Ferner spielt auch



die Art der betroffenen Region eine Rolle. So ist in der Stadt vermutlich die Selbsthilfefähigkeit geringer als auf dem Land, jedoch sind die öffentlichen Hilfeleistungspotenziale größer (Reichenbach et al., 2008, S. 23). Zudem sind insbesondere ältere Menschen (Personen ab 60 Jahren) besonders anfällig gegenüber Stromausfällen, da diese im Notfall häufig schlechter in der Lage sind, sich selber zu evakuieren (Birkmann et al., in Druck).

Besonders problematisch ist in diesem Zusammenhang die Wahrnehmung der Bevölkerung, die sich ihrer Verwundbarkeit gegenüber dem Ausfall von KRITIS oftmals nicht bewusst ist. Dies liegt vor allem daran, dass von der Gesellschaft viel in Sicherheitssysteme der Infrastruktur investiert wird, sodass die Zuverlässigkeit der Infrastrukturdienstleistungen vorausgesetzt und nicht mit Ausfällen gerechnet wird. Dieses Phänomen wird auch als *Aufmerksamkeitsparadoxon* bezeichnet. Das gefährliche in diesem Zusammenhang ist aber, dass mit der zunehmenden Komplexität der KRITIS immer kleinere Störungen weitreichende Folgen in vielen Bereichen anderer KRITIS und der Bevölkerung haben können. In diesem Zusammenhang wird dann vom *Verwundbarkeitsparadoxon* gesprochen. Verstärkt wird dieses Verwundbarkeitsparadoxon dadurch, dass heutzutage in nahezu allen Lebensbereichen elektrische beziehungsweise elektronische Geräte verwendet werden und die Abhängigkeiten von Strom daher immer weiter anwachsen[22] (siehe Abbildung 25). (Lauwe & Riegel, 2008, S. 119; BMI, 2009, S. 8)

Insgesamt gesehen existieren in der Gesellschaft stabile Mechanismen, um unerwünschte Ereignisse, gegenüber denen sie verwundbar ist, auszublenden. Weichselgartner (2000) spricht sogar davon, dass in Regionen, in denen Gefahren längere Zeit nicht aufgetreten sind, vielfach eine Art „Gedächtnisverlust“ bezüglich der Bedrohung entsteht. Dieser Mechanismus dient dem Selbstschutz, um nicht ständig ein potentiell bedrohliches Ereignis anzunehmen. Dies heißt wiederum, dass in den Teilen der Erde, in denen bedrohliche Ereignisse regelmäßiger und im Zusammenhang mit Verlusten auftreten, die Erinnerungen an diese präsenter sind und somit auch das Bewusstsein für die Verwundbarkeit stärker vorhanden ist. In der Vergangenheit wurden unter anderem in Deutschland eingetretene Ereignisse wie beispielsweise Extremhochwasser an Gedenktafeln, auf Münzen oder durch den Buß- und Bettag festgehalten, um das Bewusstsein für die Gefahr bei den Menschen aufrecht zu erhalten. Diese Symbole oder gar Feiertage haben jedoch heutzutage stark an Bedeutung und

[22] Um Beispiele für diese heranwachsende Bedeutung von elektronischen Geräten aufzuzeigen sollen im Folgenden statistische Angaben für einige wenige elektronische Geräte gemacht werden: Statistisch gesehen besitzen 95,9% der deutschen Haushalte einen Fernseher, 99,5% der Haushalte besitzen ein Telefon und 62,9% der Haushalte verfügen über einen stationären PC während 40,0% der Haushalte einen mobilen PC (Notebook, Laptop, Palmtop) besitzen. 71,9% der Haushalte verfügen über eine Mikrowelle und 68,9% der Haushalte besitzen einen Internetzugang usw. (Statistisches Bundesamt Deutschland, 2009).



Wirkung verloren und somit das Wissen um die eigene Verwundbarkeit schwinden lassen (Weichselgartner, 2000, S. 126 ff).

Bezogen auf die Wahrnehmung der Bevölkerung gegenüber Stromausfällen hat eine Schweizer Forschergruppe um Matthias Holenstein Bürger in Zürich zu ihrer Wahrnehmung hinsichtlich des Szenarios Stromausfall befragt[23]. Dabei kann einleitend festgestellt werden, dass das Wissen und auch das Interesse der Bürger gegenüber der Stromversorgung gering ist. Zwar wird der mögliche Ausfall von Kühlschränken oder Kühltruhen, der Ausfall des Lichts sowie die fehlende Kommunikation zur Außenwelt als mögliche Folge erkannt, jedoch wird ein Stromausfall nicht als Bedrohung empfunden. Auch werden kleinere Stromausfälle schnell wieder vergessen, sodass kaum Vorbereitungen hinsichtlich eines potentiellen Stromausfalls getroffen werden. Vielmehr wird ein Stromausfall teilweise auch als positives Ereignis angesehen, da durch die starke Abhängigkeit von elektronischen Gerätschaften der Alltag für die Zeit des Stromausfalls entschleunigt wird. Anders wird ein potenzieller Stromausfall jedoch wahrgenommen, wenn Leben und Gesundheit direkt betroffen wären, wie beispielsweise bei Patienten in Krankenhäusern oder pflegebedürftige Menschen. Hier stellt der Stromausfall eine direkte Bedrohung dar. Schließlich ist zu erwähnen, dass Frauen Stromausfälle generell anders wahrnehmen als Männer. Während Frauen ihre Kenntnisse zum Umgang mit Technik im Vergleich mit Männern häufig als gering einschätzen, gehen sie auch davon aus einen Stromausfall schlechter bewältigen zu können. Auch kann man Unterschiede in der Wahrnehmung verschiedener Altersgruppen erkennen. Junge Menschen sehen durch einen Stromausfall vor allem den öffentlichen Raum, ältere Menschen vorwiegend ihre Wohnung bedroht. Dies hängt mit den Radien und Lebenswelten dieser Gesellschaftsgruppen zusammen. Während junge Menschen größere Radien im öffentlichen Raum haben, sind ältere Menschen vor allem auf ihre Wohnung als Aktionsradius fokussiert. (Holenstein, 2007, S. 7 ff)

Betrachtet man die Akzeptanz der Bürger gegenüber Stromausfällen, so wurde festgestellt, dass diese hoch ist, wenn der Ausfall trotz einer ordnungsgemäßen Wartung aufgetreten ist. Anders verhält sich dies bei ungenügendem Unterhalt der Netzinfrastrukturen, bei dem für einen Stromausfall kein Verständnis aufgebracht wird (Holenstein, 2007, S. 15).

An dieser Stelle muss verdeutlicht werden, dass die hier vorgestellten Ergebnisse durch eine Befragung der in der Stadt lebenden Bevölkerung gewonnen wurden und daher auch erst einmal nur auf diese zutreffen. Dennoch kann abschließend festgestellt werden, dass auf den Bevölkerungsschutz die immer weiter wachsende Aufgabe

[23] Die im folgenden vorgestellten Ergebnisse sind zwar in der Schweiz erhoben worden, jedoch wird an dieser Stelle davon ausgegangen, dass sich die Kulturkreise zwischen der Schweiz und Deutschland sehr ähneln sodass diese Ergebnisse auch auf Deutschland übertragen werden können.



zukommt, das Bewusstsein der Bevölkerung gegenüber ihrer Vulnerabilität bei einem Stromausfall zu sensibilisieren.

## 5.3 Erfassung der Komplexität

Wie eingangs in diesem Kapitel beschrieben, sind immer mehr Infrastrukturen auf eine zuverlässige Stromversorgung angewiesen und auch die Abhängigkeit der Bevölkerung nimmt weiter zu. Jedoch wird auch die Elektrizitätsversorgung selbst durch die zunehmende Zahl der Akteure und Komponenten immer komplexer. Komplexität wird dabei als die Schwierigkeit, Kausalzusammenhänge zwischen einer Vielzahl von Ursachen und beobachteten Wirkungen zu identifizieren und zu qualifizieren, definiert (eigene Übersetzung in Anlehnung an IRGC, 2005, S. 77). Diese Komplexität ist dabei häufig von gegenseitigen Abhängigkeiten, sogenannten Interdependenzen, geprägt. Bezogen auf unterschiedliche Infrastrukturdienstleistungen wird diese Abhängigkeit, wie Abbildung 26 zeigt, von Lauwe und Riegel (2008) dargestellt:

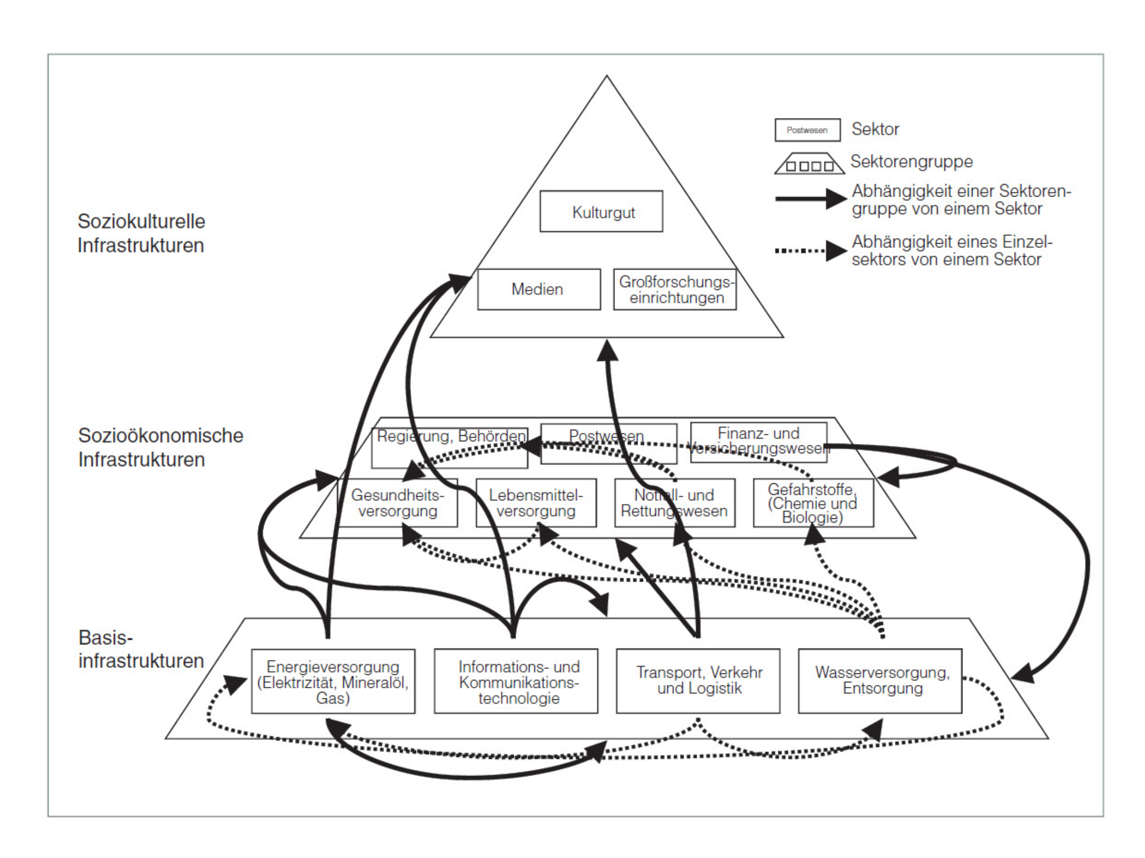



**Abbildung 26: Interdependenzen von Basis-, sozioökonomischen und soziokulturellen Infrastrukturen**

Quelle: (Lauwe & Riegel, 2008, S. 119)



Interessant ist aber neben der grundsätzlichen Interdependenz von Infrastrukturdienstleistungen auch die Kenntnis über Charakteristika dieser Abhängigkeiten. In einem ersten Ansatz zur Erfassung der Interdependenzen unterscheiden Rinaldi et al. (2001) vier verschiedene Arten der Interdependenz:

(i) Physische Interdependenz: Beide Infrastrukturen sind von Gütern abhängig, die die jeweils andere liefert, wie beispielsweise Bahn und Kohlekraftwerken, die jeweils Energie, bzw. Kohle benötigen.

(ii) Cyber-Interdependenz: Die Infrastruktur ist von Informationen abhängig, die eine andere Infrastruktur bereitstellt.

(iii) Geographische Interdependenz: Durch die geographische Nähe sind beispielsweise bei einem Naturereignis sofort mehrere Infrastrukturkomponenten und damit Prozesse betroffen.

(iv) Logische Interdependenz: Es besteht zwischen zwei Infrastrukturen eine Verbindung, die nicht durch die drei erstgenannten beschrieben werden kann. Häufig spielen hier durch Menschen getroffene Entscheidungen eine Rolle.

Neben diesen gegenseitigen Abhängigkeiten benennen Rinaldi et al. (2001) zudem einige weitere „Dimensionen zur Beschreibung von Interdependenzen“, die in Abbildung 27 dargestellt sind:

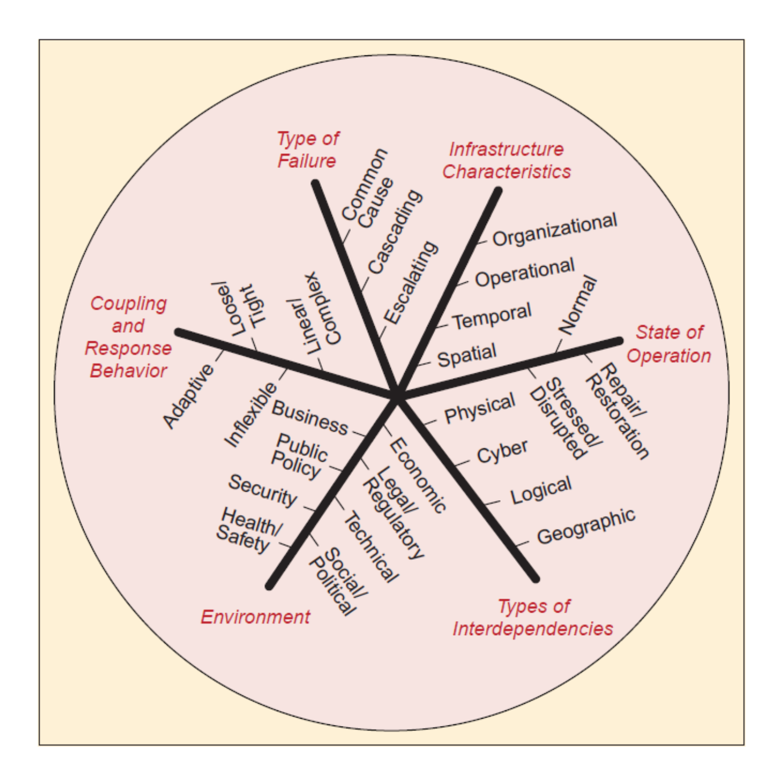



**Abbildung 27: Dimensionen der Interdependenzen Kritischer Infrastrukturen**

Quelle: (Rinaldi et al., 2001, S. 12)



Demnach werden neben den verschiedenen Arten der Interdependenz auch das Umfeld (z.B. gesetzliche oder ökonomische Rahmenbedingungen), der Betriebszustand (z.B. normal oder in Reparatur), die Charakteristika der Infrastruktur (z.B. Organisationsstruktur), die Art des Fehlers und das Kopplungs- und Rückmeldeverhalten der Infrastruktur als Dimensionen der Interdependenzen verstanden[24]. Problematisch ist hierbei jedoch, dass lediglich die Art der Interdependenz und das Kopplungs- und Rückmeldeverhalten der Infrastrukturen als Beschreibungsversuch der Abhängigkeit verstanden werden können. Alle anderen Dimensionen sind vielmehr als zusätzliche, äußere Faktoren zu bewerten, die zwar einen Einfluss auf die Auswirkungen eines Stromausfalles haben oder ihn begünstigen können, jedoch nicht das Zusammenspiel verschiedener Komponenten oder Infrastrukturdienstleistungen erläutern.

Ferner lassen Rinaldi et al. auch offen, welche Konsequenz sich aus den verschieden Arten der Interdependenz ergibt. Hierdurch bleibt die Beschreibung der Abhängigkeiten sehr abstrakt und wenig zielführend im Sinne der Verwundbarkeitsreduktion.

Allerdings ist es sinnvoll, die auch von Rinaldi et al. (2001) beschriebenen, Fehlerarten zu betrachten. Zwar beschreiben diese nicht die Interdependenzen, stellen jedoch einen Aspekt der Komplexität dar, indem zwischen einer gemeinsamen Ursache der Ausfälle, Kaskadeneffekten und eskalierenden Ursachen unterschieden wird. Kaskaden entstehen dabei dann, *„wenn eine Störung oder ein Ausfall in einer Infrastruktur Folgen hat, die sich auf eine weitere Infrastruktur auswirken."* (Schulze, 2006, S. 124) Eskalierende Effekte verstärken sich gegenseitig, obwohl sie unabhängig voneinander entstanden sind (Schulze, 2006, S. 124). Letztere Art der Ursachen scheint auf den ersten Blick häufig der Grund für Stromausfälle zu sein (vgl. Kapitel 4.1.3 und Tabelle 4). Hier wäre jedoch eine tiefgehende Analyse bezüglich Ursachen, Abhängigkeiten und eingetretenen Folgen nötig, um eine Einschätzung über Ursache-Wirkungs-Gefüge treffen zu können.

Durch die vielfältigen Abhängigkeiten, Einflussfaktoren und Interdependenzen verschiedener KRITIS, die bisher kaum wissenschaftlich behandelt worden sind, und der damit verbundenen Komplexität des Systems ist die Erfassung möglicher Effekte, die je nach Art und Intensität des Ereignisses verschieden sind, nahezu unmöglich. Gesicherte Methoden, um den Gesamtschaden von Ausfällen oder Störungen Kritischer Infrastrukturen zu ermitteln, bestehen bislang nicht. Dabei lassen sich weder die volle Zahl von Abhängigkeiten noch deren Folgen genau abschätzen (Schulze, 2006, S. 126 f). Zwar versuchen Forscher dies zu modellieren, doch die Ursache-Wirkungs-Komplexität bei Störungen und Ausfällen ist mittelfristig beinahe nicht zu lösen (Schulze, 2006, S. 125 ff), da Verknüpfungen und Interdependenzen häufig nur

[24] Die verschiedenen Dimensionen werden in Anhang 1 ausführlicher erläutert.



qualitativ zu erfassen sind und sich viele logische und physische Verknüpfungen erst bei einem Ereignis wirklich offenbaren (Lauwe & Riegel, 2008).

Bouwmans et al. (2006) unterscheiden zwischen *physischer* und *sozialer* Netzwerkkomplexität. Während sich die physische Netzwerkkomplexität aus der Menge der Verknüpfungen verschiedener Komponenten ergibt, ist die soziale Netzwerkkomplexität durch Menschen, Institutionen und Unternehmen geprägt. Beide Bereiche unterliegen ständigen Veränderungen, beispielsweise durch technischen Wandel oder Privatisierung und Marktliberalisierung. Dennoch muss ihr Zusammenspiel funktionieren, damit die Stromversorgung gewährleistet ist. Eine tiefergehende Analyse bezüglich des Zusammenspiels der verschiedenen Akteure und Komponenten wäre in diesem Zusammenhang sinnvoll.

Eine solche Analyse, die sowohl die Interdependenzen von KRITIS als auch die Ursachen und Auswirkungen in den USA untersuchte, wurde von Zimmermann (2004) durchgeführt. Für eine Datenbankanalyse von Ausfällen wurden folgende Kriterien gewählt:

- Typen von Infrastrukturkomponenten, die andere Komponenten beschädigt haben
- Typen von Infrastrukturkomponenten, die durch Schäden in anderen Komponenten beschädigt wurden
- Der Zusammenhang zwischen Ursache und Wirkung des Fehlers
- Die häufigsten Ursache/Fehler Kombinationen
- Anzahl der betroffenen Personen und Art der Betroffenheit

Allerdings beinhaltete diese Untersuchung nur einige ausgewählte Infrastrukturkomponenten und vernachlässigt zudem Terroranschläge und Naturgefahren. Eine solche Analyse könnte für Deutschland sinnvoll sein, wofür eine umfangreiche und konzernübergreifende Datenbank der aufgetretenen Störfälle die Grundlage sein müsste.

Abschließend kann festgehalten werden, dass die Komplexität der Elektrizitätsversorgung und mögliche Wechselwirkungen mit anderen KRITIS-Bereichen bislang nicht hinreichend erfasst sind. So kann beispielsweise keine Aussage dazu gemacht werden, ob bestimmte Komponenten oder Interdependenzen besonders häufig betroffen sind. Fraglich ist, ob ein tieferes Verständnis der Abläufe bei Stromausfällen aufgrund der geringen Zahl ihres Auftretens (siehe Kapitel 5.4) und der zumeist rückblickend qualitativen Bewertung (Lauwe & Riegel, 2008) überhaupt möglich ist. Hier besteht in Zukunft starker Handlungsbedarf, um den Wissensstand über sich abzeichnende Risiken und Optionen zur Beherrschung zu verbessern (Odenthal, 2003, S. 301).



## 5.4 Analyse der Ausfälle der Vergangenheit

Um einen ersten Überblick über das Wesen der Störfälle in Deutschland zu bekommen, werden in diesem Abschnitt Daten zur Versorgungssicherheit, vergangener Stromausfälle sowie deren Ursache und Auswirkungen in Deutschland analysiert.

Grundsätzlich unterliegt jeder Strombetreiber per Gesetz[25] der Verpflichtung, Daten zu Störungen oder Ausfällen sowie deren Ursache und Ausmaß der Bundesnetzagentur vorzulegen (Bundesnetzagentur, 2009, S. 126). Eine Störung liegt nach Auffassung der Bundesnetzagentur vor, sobald die Versorgung eines oder mehrerer Letztverbraucher oder Weiterverteiler länger als eine Sekunde unterbrochen wird (VDN, 2007, S. 20). Mit Hilfe der vorhandenen Daten wird unter anderem der *System Average Interruption Duration Index* (SAIDI) – der Wert für die Versorgungsqualität – nach international anerkannten Methoden für Deutschland berechnet (Bundesnetzagentur, 2009, S. 126). Dieser Wert beschreibt die durchschnittliche Versorgungsunterbrechung in Minuten je angeschlossenem Letztverbraucher. Folgende Tabelle 5 zeigt die Entwicklung der mittleren Nichtverfügbarkeit in den letzten Jahren.

**Tabelle 5: Gesamtübersicht der mittleren Nichtverfügbarkeit je Netzkunde und Jahr (SAIDI)**

| | Allgemeindaten | | Niederspannung | | Mittelspannung | | SAIDI |
|---|---|---|---|---|---|---|---|
| Berichtsjahr | Anzahl Netzbetreiber/Netze | Letztverbraucher (in Mio.) | Anzahl Unterbrechungen (insg. in Tsd) | SAIDI (Minuten) | Anzahl Unterbrechungen (insg. in Tsd) | SAIDI (Minuten) | SAIDI (Minuten) |
| 2008 | 813/834 | 48,4 | 171,5 | 2,57 | 36,6 | 14,32 | 16,89 |
| 2007 | 825 | 48,5 | 196,3 | 2,75 | 39,5 | 16,50 | 19,25 |
| 2006 | 781 | 48,5 | 193,6 | 2,86 | 34,4 | 18,67 | 21,53 |

Quelle: (Bundesnetzagentur, 2010)

Die kontinuierliche Verbesserung des Stromversorgungsnetzes in Deutschland von 2004 (22,9 min/a) (Bundesnetzagentur, 2006b) bis hin zu 16,89 min/a im Jahr 2008, zeigt sich auch im langjährigen Vergleich. In Abbildung 28 sind die Störungen mit Versorgungsunterbrechungen im Mittelspannungsnetz seit 1994 aufgelistet und nach Ursache untergliedert. Neben der allgemeinen Reduzierung der Störungen seit 1994 fällt auf, dass die „Atmosphärischen Einwirkungen“, insbesondere durch Naturgefahren, im Vergleich zu den Jahren 2000 und 2001 im Jahr 2007 deutlich gestiegen sind. Zu diesem Resultat hat besonders der Orkan „Kyrill“ im Jahr 2007 beigetragen. Stellt man die Ergebnisse der mittleren Nichtverfügbarkeit in den europäischen Vergleich[26],

[25] Nach § 52 EnWG müssen Betreiber von Energieversorungsnetzen bis zum 30. Juni eines Jahres über alle im letzten Kalenderjahr in ihrem Netz aufgetretenen Versorgungsunterbrechungen Bericht erstatten (Bundesnetzagentur, 2009, S. 126).

[26] (VDE, 2010)



herrscht in Deutschland sehr hohe Versorgungssicherheit (99,996%) (VDE, 2010; Bundesnetzagentur 2008).

Wichtig zu beachten ist, dass bei den Untersuchungen der Versorgungsunterbrechungen oftmals nur die Bereiche Niederspannung (NS) und Mittelspannung (MS) betrachtet werden. Dies hat den Grund, dass Störungen im Hoch- und Höchstspannungsnetz als Rückwirkungen auf der Mittelspannungsebene registriert werden (VDN, 2006, S. 27). Daher ist die MS-Ebene jene mit der längsten Versorgungsunterbrechung pro Jahr (siehe Tabelle 5) und folglich in den Untersuchungen von besonderer Relevanz (siehe Abbildung 28).

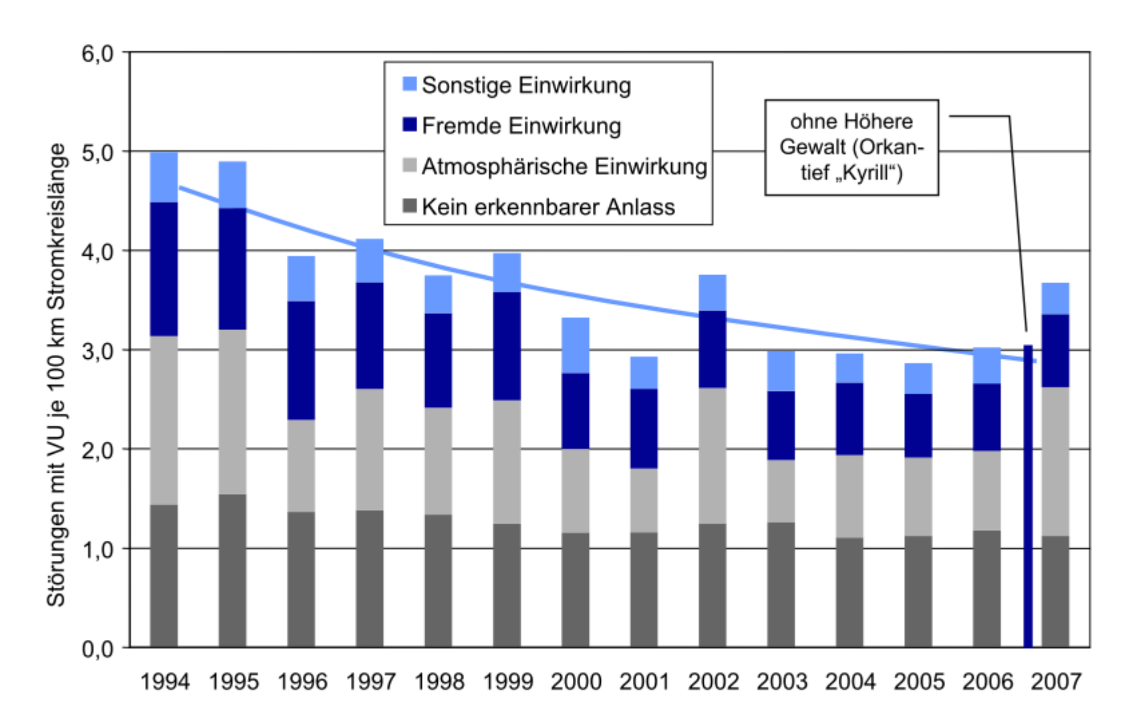



**Abbildung 28: Störungen mit Versorgungsunterbrechungen im Mittelspannungsnetz**

Quelle: (Schubert et al., 2008)

Die Versorgungsunterbrechungen werden prinzipiell durch den Verband der Netzbetreiber (VDN) in vier Gruppen eingeteilt: Störungen durch fremde, atmosphärische und sonstige Einwirkung, sowie Störungen ohne erkennbaren Anlass. Atmosphärische Einwirkungen beinhalten dabei ausschließlich natürliche/wetter-bedingte Einflüsse wie beispielsweise Gewitter, Sturm, Eis, Eisregen, Schnee, Raureif, Nebel, Betauung, eingedrungene Feuchtigkeit bei Regen, Schneeschmelze, Hochwasser, Kälte, Hitze oder Ähnliches. In der Kategorie Fremde Einwirkung werden Störungen durch Personen (Berührung oder Annäherung an spannungsführende Teile), Tiere, Bäume, Erd- und Baggerarbeiten, Brand, Kräne, Fahrzeuge, Flugobjekte (Drachen,



Ballone, Flugzeuge oder Ähnliches) zusammengefasst. Zusätzlich zu den vier Gruppen existiert das Merkmal *höhere Gewalt.*

> *„Hierbei handelt es sich um ein betriebsfremdes, von außen durch außergewöhnliche elementare Naturkräfte oder durch Handlungen dritter Personen herbeigeführtes Ereignis, das nach menschlicher Einsicht und Erfahrung unvorhersehbar ist, mit wirtschaftlich vertretbaren Mitteln und durch äußerste, nach der Sachlage vernünftigerweise zu erwartende Sorgfalt nicht verhütet und unschädlich gemacht werden kann und auch nicht wegen seiner Häufigkeit vom Betriebsunternehmer in Kauf zu nehmen ist. Unter Höhere Gewalt fallen insbesondere außergewöhnliche Naturkatastrophen (z.B. Hochwasser mit Auswirkungen der Oderflut im Jahre 1997), Streik, gesetzliche und behördliche Anordnung, Terroranschläge oder Krieg.“* (VDN, 2007, S. 37).

Interessant für potentielle Handlungsoptionen zur Verringerung der Verwundbarkeit der Elektrizitätssysteme ist auch die Frage, wo Störungen am häufigsten auftreten. Abbildung 29 zeigt, dass Freileitungen zwar den geringeren Anteil an der Stromkreislänge besitzen, jedoch Hauptursache der Nichtverfügbarkeit von Strom sind. Hier ist das System folglich besonders Verwundbar.

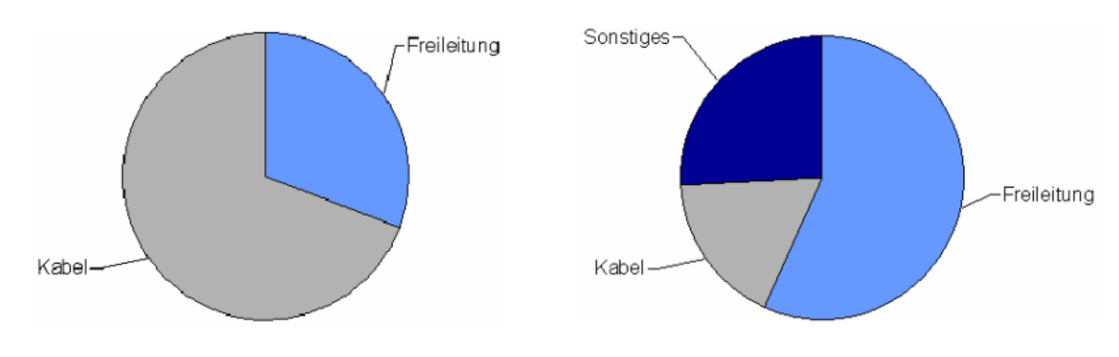



**Abbildung 29: Ursächliche Komponenten für Stromausfälle**

Quelle: (Schubert et al., 2008)

Eine Quantifizierung der Kosten eines Stromausfalls bzw. Zwischenfalls ist dagegen erheblich schwieriger. Aufgrund der enormen Vernetzung sind die wirtschaftlichen Folgen eines Stromausfalls nur bedingt messbar. Ajodhia (2006) beschreibt die Kosten einer Unterbrechung als das Zusammenspiel zweier Variablen. Einerseits die Art des Ausfalls, andererseits der Umgang mit einem Störfall. Besonders die Art des Netzwerkes und das Notfallmanagement des Stromversorgungssystems, beeinflussen den Umfang des Störfalls und folglich die entstandenen Kosten. Grundsätzlich gibt es



zwei Methoden, die Kosten eines Stromausfalls zu messen: die direkte und die indirekte Bemessung. Die direkte Erfassung der Kosten erfolgt über

- Daten vergangener Ausfälle und deren Kosten,
- Befragung betroffener Verbraucher und deren Einschätzung entstehender Kosten im Falle eines Stromausfalls, sowie
- Bewertung der Ausfallsicherheit durch die Verbraucher (Investition in höhere Sicherheit oder geringere Sicherheit akzeptieren)

Andere Methoden versuchen dagegen die Kosten indirekt zu bemessen. Beispielsweise liefert das Bruttonationaleinkommen in Verbindung mit der konsumierten Elektrizität die Obergrenze der Kosten. Die Untergrenze ergibt sich durch den Strompreis in Verbindung mit dem Verbrauch (Ajodhia, 2006).

## 5.5 Zwischenfazit des Systems „KRITIS-Mensch“

Kapitel 5 hat verdeutlicht, dass sich die Verwundbarkeit der Kritischen Elektrizitätsversorgung direkt auch auf andere KRITIS und die Bevölkerung auswirkt. Da letztere jedoch zunehmend auf die Zuverlässigkeit der Stromversorgung vertraut und schlecht vorbereitet ist, sind die Auswirkungen im Ereignisfall umso gravierender. Auch besteht neben der systeminternen Komplexität, die insbesondere durch die Vielzahl der Akteure und Komponenten bestimmt wird, auch eine Gesamtkomplexität. Umso wichtiger ist es hierbei, die Komplexität der Zusammenhänge und Abhängigkeiten im System der Elektrizitätsversorgung selbst und den von ihr abhängigen weiteren Bereichen zu verstehen. Hierzu gibt es jedoch bisher kaum Ansätze. Zwar haben Rinaldi et al. (2001) eine erste Klassifikation entwickelt, die jedoch wenig präzise und im Rahmen der Verwundbarkeitsreduktion wenig zielführend ist. Um diese Lücke zu überbrücken, könnte die Analyse vergangener Störfälle sinnvoll sein. Ein erster Überblick zeigt, dass die Gesamtdauer und Anzahl der Störfälle in den letzten Jahren zurückgegangen ist, die atmosphärischen Einwirkungen jedoch immer wieder (wie im Jahr 2007) Hauptauslöser für Unterbrechungen im Mittelspannungs-Bereich sein können, wo insgesamt die meisten Störungen auftreten, wobei Freileitungen, trotz ihrem verhältnismäßig kleinen Anteil an der Stromkreislänge, die am häufigsten betroffenen Komponenten sind.



# 6 Staatliche und privatwirtschaftliche Handlungsmöglichkeiten zur Förderung der Resilienz Kritischer Infrastrukturen

Anlehnend an die Analyse der Verwundbarkeit der Elektrizitätsversorgung anhand der Komponenten *Exposition*, *Anfälligkeit* und *Bewältigungskapazität*, können Handlungsmöglichkeiten aufgezeigt werden. Ziel ist es, Exposition und Anfälligkeit zu reduzieren und die Bewältigungskapazität des Systems zu erhöhen.

| f (Vulnerabilität) = Exposition (Hazard), Anfälligkeit, Bewältigungskapazität |
|---|

Das Konzept der Vulnerabilität ist eher eine Beschreibung eines Prozesses als eines Status Quo und unterstreicht dabei die Möglichkeit zum Handeln (siehe beispielsweise Blaikie et al., 1994; Wisner et al., 2004; Birkmann, 2006). Die Einbeziehung von Akteuren, die in den Prozess eingreifen, um die Verwundbarkeit zu reduzieren ist dabei von besonders hoher Relevanz. Um dies im Falle der Vulnerabilität von Kritischer Elektrizitätsinfrastruktur auch umsetzbar zu machen, sollen im Folgenden ausgewählte Möglichkeiten des Staates und der Privatwirtschaft aufgezeigt werden, die die Verwundbarkeit reduzieren können .

## 6.1 Exposition

Die Möglichkeiten zur Reduktion der Exposition unterscheiden sich, ebenso wie die Exposition selbst, nach Art der Gefahr, weshalb auch hier zwischen Naturgefahren und kriminellen Handlungen unterschieden wird.

### 6.1.1 Exposition gegenüber Naturgefahren

Die Reduktion der Exposition von Komponenten gegenüber Naturgefahren hängt von ihrer räumlichen Abgrenzbarkeit ab. Während hochwasserexponierte Gebiete mittels GIS und der Wahl verschiedener Hochwasserszenarien relativ klar definiert werden können (siehe beispielsweise Birkmann et al., in Druck), sind Hitzewellen oder Stürme kaum eingrenzbar. So erstreckte sich die Hitzewelle im Jahr 2003 über ganz Europa (BfG, 2006; Koppe, 2004). Jedoch macht das Ergreifen von Maßnahmen zur Reduktion der Exposition nur Sinn, wenn auch das Auftreten räumlich klar begrenzt werden kann, wie beispielsweise bei Hochwasser. Hier können exponierte Komponenten identifiziert und ggf. aus dem Überschwemmungsgebiet verlegt oder geschützt werden. In diesem Zusammenhang macht eine Verwundbarkeitsanalyse der einzelnen Komponenten und ihrer Bedeutung für den jeweiligen Prozess Sinn, um eine Kosten-Nutzen Abwägung zu gewährleisten (siehe hierzu Krings, in Druck).



Außerdem werden durch die Energieversorgungsunternehmen Maßnahmen getroffen, um Vorsorge gegenüber Extremereignissen zu betreiben. Dabei ist unter anderem der Anteil an Erdkabelstrecken im europäischen Vergleich recht hoch, wodurch der Schutz gegenüber Starkwind sowie Schneebelastung ausgebaut wird. Desweiteren werden Notwasseranschlüsse für Kraftwerke errichtet, um die Flusswasserkühlung auch in Hitzeperioden zu gewährleisten. Schließlich sind innerhalb der Energieversorgungsunternehmen Krisenstäbe vorhanden, *„um bei extremen Wetterereignissen eine schnelle Reaktion auf Schäden und Ausfälle möglich zu machen*“ (Die Bundesregierung, 2008, S. 35).

### 6.1.2 Exposition gegenüber kriminellen Handlungen

Die Handlungsmöglichkeiten bzgl. des Herabsetzens der Exposition gegenüber kriminellen Handlungen werden in Anlehnung an Kapitel 4.1.2 in Maßnahmen gegen Terroranschläge und Cyberattacken unterschieden.

#### Terroranschläge

Im Allgemeinen können die Bewältigungs- bzw. Schutzmaßnahmen gegenüber terroristischen Anschlägen in *physische*, *personelle* sowie *organisatorische Maßnahmen* unterteilt werden, wobei diese je nach Komponente der Elektrizitätsversorgung unterschiedlich ausfallen. Unter *physischen Schutzmaßnahmen* sind vor allem bauliche Veränderungen bzw. Verbesserungen von Anlagen, wie beispielsweise überwachte Umzäunungen, Videoüberwachung, Torkontrollen, Bewegungsmelder, Betonelemente, die Härtung von Anlagen, etc. zu verstehen, was insbesondere für alle Arten von Kraftwerken und teilweise auch Transformatoren-Stationen zutrifft (BMI, 2005, S. 21 f).

Für den Schutz von Atomkraftwerken in Deutschland existieren zwei unterschiedliche Ansätze. So zum einen das „Einnebeln[27]“ der Kraftwerke bei Annäherung eines Flugzeuges, was zwar eine kostengünstige Schutzvariante ist, jedoch erhebliche Probleme mit sich bringt. Flugstraßen sind oftmals zu nahe an den Kraftwerken, bestimmte Wetterbedingungen müssen vorherrschen und einfache GPS-Geräte orten das Ziel auch ohne freie Sicht. Zum anderen können AKWs weitaus effektiver durch sogenannte Beton-Gitterwände in den möglichen Einflugschneisen geschützt werden. Diese sollen, in bestimmter Entfernung (50 m) zum Reaktor aufgestellt, den Angriff einer Passagiermaschine abwehren (Kuhn & Neuneck, 2005, S. 25 f).

[27] Nebelwefer im Umkreis des zu schützenden Kraftwerkes schießen Nebelgranaten ab, sobald sich ein Flugzeug bis auf 15 Km nähert, um das Kraftwerk mit „Nebel“ zu umhüllen und für den „angreifenden“ Piloten unsichtbar werden zu lassen (Kuhn & Neuneck, 2005, S. 25).



*Personelle Maßnahmen* beinhalten die Sensibilisierung der Beschäftigten durch Seminare und Schulungen. Derartige Schulungen werden beispielsweise auf EU-Ebene im Rahmen des Zivilschutzmechanismus für nationale Teamleiter und Sachverständige konzipiert. Seit dem Jahr 2002 finden auf EU-Ebene auch umfangreiche Simulationsübungen[28] statt, die speziell auf terroristische Szenarien zugeschnitten sind (EU-Kommission, 2004, S. 4 f). Im *organisatorischen Bereich* können beispielsweise Ausweiskodierung, Sicherheitskontrollen oder das Bereitstellen von Alarmplänen für Anschläge oder Explosionen für mehr Sicherheit sorgen (BMI, 2005, S. 21 f).

Die eher allgemeinen Schutzmaßnahmen sind grundsätzlich von hoher Bedeutung. Im Hinblick auf terroristische Anschläge sowie deren Bewältigungskapazität stehen Präventivmaßnahmen zum Schutz der Bevölkerung und der Beseitigung der Ursachen des Terrorismus im Vordergrund (Hanning, 2008, S. 41). Jedoch gelten Terroranschläge grundsätzlich als schwer vorhersehbar. *„Zwar handeln Terroristen nicht zufällig, aber um den größtmöglichen Effekt zu erzielen, greifen sie überraschend an, wodurch die Anschläge für ihre Opfer [...] zufällig sind“* (Benzin, 2005, S. 222 f).

### Cyberattacken

Wie der Bericht der Schutzkommission des Bundesministeriums des Innern (BMI, 2003) feststellt, können Schädigungen Kritischer Infrastruktur durch Cyberattacken auch zukünftig nicht ausgeschlossen werden. Die Abhängigkeiten von Informations- und Kommunikationstechnologien werden in Zukunft weiter zunehmen, wobei die steigende Komplexität der Technologien tendenziell dazu führen wird, dass diese fehler- und störanfälliger werden. Um etwa zu verhindern, dass die Prozess-steuerungstechnik von Energieversorgern manipuliert werden kann, ist es wichtig, Soft- und Hardware so weiterzuentwickeln, dass ein weitestgehend störungsfreier Betrieb möglich ist. Gleichzeitig muss die Systemredundanz so ausgebaut werden, dass auch bei Störungen die Handlungsfähigkeit erhalten bleibt[29] (Reichenbach et al., 2008).

Da die Bedrohungslage von Cyberattacken nach wie vor unklar ist (siehe auch Kapitel 0) und hier weiterer Forschungsbedarf erkannt wurde (Schulze, 2006), ist die Durchführung von Planspielen und Simulationen sinnvoll.[30]

---

[28] Bisher hat es drei Übungen gegeben, welche auf terroristische Szenarien zugeschnitten waren: „Euratox“ (Oktober 2002 in Frankreich), „Common Cause“ (Oktober 2002 in Dänemark) und die EU-Reaktionsübung (Januar 2003 in Belgien) (EU-Kommission, 2004, S. 5).

[29] Weitere detaillierte, insbesondere technische Schutzmaßnahmen zur IT-Sicherheit, finden sich in den „IT-Grundschutzkatalogen“ sowie der Publikation „Kommunikations- und Informationstechnik 2010+3: Neue Trends und Entwicklungen in Technologien, Anwendungen und Sicherheit“ herausgegeben vom BSI.

[30] Beispielsweise wurde von der National Security Agency (NSA) in den USA die Übung *Eligible Receiver* durchgeführt. In Deutschland fand 2001 das Planspiel (*Cyber Terror Exercise* – CYTEX) unter Beteiligung zahlreicher staatlichen und privatwirtschaftlicher Organisationen statt. Im US-amerikanischen



**Software-Sicherheit**

Wenn auch Technik nicht alleine für Sicherheit sorgen kann, muss festgehalten werden, dass es ohne Technik keine Sicherheit geben kann (Schulze, 2006). Hierzu gehört insbesondere die Software-Sicherheit. Problematisch ist, dass Betreiber von KRITIS oftmals von Beginn an auf unsichere Technik angewiesen sind. So bringt der Einsatz von off-the-shelf Produkten, die Schwachstellen in der Softwaresicherheit nur reaktiv beheben, ein erhebliches Risikopotential mit sich. Diese lässt sich jedoch schon aus Kostengründen kurzfristig nicht ersetzen. Daher ist neben der Privatwirtschaft auch der Staat angehalten, den Bereich der Forschung und Entwicklung sicherer Software-produkte zu unterstützen und entsprechende Projekte zu fördern (Schulze, 2006; Kuhn, 2005).

**SCADA-Systeme und Sicherheit**

Wie in Kapitel 0 dargestellt, wird seit längerem im verstärkten Maße diskutiert, dass sich SCADA-Systeme zukünftig als Angriffsziele für Cyberattacken eignen könnten (Kuhn, 2005). Hierbei können Internetschnittstellen für den Zugang zu SCADA-Systemen genutzt werden, um diese anschließend „fernzusteuern" (Kuhn, 2005; Schulze, 2006). Dabei ist es bei der Entwicklung neuer Prozessleittechniken von besonderer Bedeutung, Sicherheitsaspekte zu berücksichtigen. Dies wird durch den vor kurzem im Iran aufgetauchten *Stuxnet-Trojaner* verdeutlicht (siehe auch Kapitel 0) (Kuhn, 2005).

**Internet und Sicherheit**

Die systemimmanenten Sicherheitsprobleme des Internets lassen Überlegungen laut werden, langfristig eine vom Internet unabhängige Kommunikationsplattform zu entwickeln. Das US-Militär entwickelt seit 2002 ein eigenes Netzwerk „Global Information Grid Bandwidth Expansion" (GIG-BE), um den militärischen Anforderungen eines Kommunikationsnetzes auch unter sicherheitsrelevanten Aspekten gerecht zu werden (Wilson, 2005). Dieses vom Internet losgelöste Netzwerk wird als Grund angeführt, warum es keine Angriffe auf relevante Informationsinfrastrukturen der US-amerikanischen Streitkräfte gegeben hat (Fischer, 2007). Vermutlich wird es jedoch kurz- oder mittelfristig nicht möglich sein, eine neue Kommunikationsplattform zur Vernetzung von KRITIS zu errichten.

**Smart Grids und Sicherheit**

Von besonderer Sicherheitsrelevanz ist die Netzwerkumstellung auf Smart Grids (siehe hierzu auch Kapitel 6.3.3). Sowohl Endverbraucher als auch Strombetreiber sehen sich

---

Planspiel *Electronic Pearl Harbor* aus dem Jahr 2002 wurden Angriffe auf SCADA-Systeme von Energieversorgern simuliert. (Kuhn, 2005; Kuhn & Neuneck, 2005)



laut Sicherheitsexperten einer vermehrt zu erwartenden Gefahr von Cyber-Angriffen ausgesetzt. Jegliche Information über die Art des Stromverbrauchs der Endverbraucher wird in den haushaltsintern installierten Smart Metern gespeichert. Allein aus Datenschutzgründen ist diese Umstellung von großer Sicherheitsbedeutung.
Stromanbieter hingegen müssen einerseits aufgrund der Sicherheitslücken im System mit Manipulationen der Smart Meter in Haushalten rechnen, was einen erheblichen wirtschaftlichen Schaden für die Unternehmen bedeuten kann. Andererseits ist mit Angriffen auf zentrale Computer der Betreiber zu rechnen, die einen großflächigen Ausfall zur Folge haben können. Maßnahmen müssen dementsprechend sowohl auf politischer Ebene, um eine klare Regelung für den Umgang mit Verbraucherdaten zu schaffen, als auch auf technischer Ebene, um die vorhandenen Sicherheitslücken zu schließen, durchgeführt werden. Dabei spielt besonders die Zusammenarbeit zwischen der Regierung und den privaten Stromanbietern eine große Rolle. Sicherheits- und Qualitätsanalysen sowie unabhängige Untersuchungen der Smart Meter müssen ausgeweitet werden. Zudem führt eine enge Zusammenarbeit zwischen Stromanbietern und Smart Meter Herstellern zur Verbesserung der Netzwerkqualität und einer effektiveren Behebung der Netzwerkfehler. (McDaniel & McLaughlin, 2009)

Grundsätzlich bleibt festzuhalten, dass man den genannten Herausforderungen nur gerecht werden kann, wenn der Schwerpunkt der staatlichen Aktivitäten auf der Unterstützung von Forschung liegt, um Schwachstellen und Störungen rechtzeitig und angemessen begegnen zu können. Von großer Wichtigkeit ist eine Bewusstseinsbildung, die, wie Untersuchungen zeigen, in deutschen Unternehmen schlecht ausgeprägt ist (vgl. BMI, 2009). Insbesondere Betreiber von Informations- und Kommunikationsnetzwerken, sowie Betreiber anderer Kritischer Infrastrukturunternehmen wie beispielsweise Stromanbieter müssen für Gefahren und Schutzmöglichkeiten sensibilisiert werden. Auch der Unterstützung der technischen Vorsorge im Sinne des Einsatzes möglichst sicherer Soft- und Hardware, bei privaten wie staatlichen Stellen, sollte zukünftig ein größerer Stellenwert beigemessen werden. Im Sinne einer Früherkennung von Cyberattacken und zur Vorbereitung des Krisenmanagements, ist es von staatlicher Seite wichtig, zu einer erfolgreichen Schutzpolitik anzuregen und Erfahrungen zu vermitteln (Schulze, 2006).

Des Weiteren sind zukünftig in einem noch stärkeren Maße die Planung und der Aufbau eines nationalen und internationalen Krisenmanagements notwendig. In diesem Zusammenhang sollten weitere Übungen mit staatlichen und privaten Stellen durchgeführt werden. Wichtig ist ebenfalls die Schaffung besserer internationaler juristischer wie praktischer Grundlagen für eine erfolgreiche Cybersecurity (vgl. Fischer, 2007, S. 173 - 183).



## 6.2 Anfälligkeit

Zur Reduktion der Anfälligkeit sollen Handlungsmöglichkeiten dargestellt werden, die den verschiedenen, in Kapitel 4.2 aufgezeigten, Einflussfaktoren entsprechen.

### 6.2.1 Institutionelle Faktoren

Durch weitreichende Privatisierungen der Elektrizitätsversorgung in vielen Ländern und die Liberalisierung des europäischen Strommarktes haben sich Veränderungen ergeben, die heute die Anfälligkeit der Versorgung erhöhen. Diese Probleme sind vielschichtig, sodass Handlungsmöglichkeiten anhand verschiedener Aspekte betrachtet werden müssen.

**Privatisierung**

Die Privatisierung der Versorgung hat in vielen Bereichen auch dazu geführt, dass die Betreiber für die Sicherheit verantwortlich gemacht werden (IRGC, 2006, S. 12). Dass die primäre Verantwortung zum Schutz der Infrastrukturen in privater Hand liegt, kann den Staat jedoch nicht von seinen Gewährleistungspflichten befreien. Es gilt hier, die Wirtschaftsinteressen mit den Allgemeininteressen zu verbinden. Zwar kann dies durch konsensuales Vorgehen geschehen, beispielsweise gilt die Erstellung des Basisschutzkonzeptes (BMI, 2005) als gelungenes Beispiel für ein Public Private Partnership (PPP) (Schäuble, 2010, S. 24), jedoch ist eine mangelhafte Umsetzung dort zu erwarten, wo wirtschaftliche und gesellschaftliche Interessen divergieren (Kloepfer, 2010, S. 17). Folglich stellt sich die Frage, in welchem Rahmen die gemeinsame Verantwortung formalisiert werden könnte, wobei sich zunächst die Europäische Union anbietet. In diesem Rahmen wurden bereits Initiativen zur Sicherheit der Netze ergriffen.[31] In diesem Zusammenhang legte die Kommission 2005 beispielsweise das Grünbuch über ein Europäisches Programm für den Schutz Kritischer Infrastrukturen (EPSKI) (KOM(2005) 576 endgültig) vor. Ihm folgten die Mitteilung der Kommission über ein Europäisches Programm für den Schutz Kritischer Infrastrukturen (KOM(2006) 786 endgültig) und schließlich die Richtlinie über die Ermittlung und Ausweisung europäischer Kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern (RL 2008/114/EG). Zwar sind hiernach die Mitgliedsstaaten und

[31] Gem. Art. 170 I AEUV (ex-Art. 154 EGV) trägt sie zum Auf- und Ausbau transeuropäischer Netze in den Bereichen der Verkehrs-, Telekommunikations- und Energieinfrastruktur bei. Gemäß Art 171 I, Spiegelstrich 1 AEUV, ist sie jedoch lediglich zum Erlass von Leitlinien ermächtigt, die keinen operativen Verpflichtungscharakter aufweisen. In diesem Zusammenhang wurde jedoch in der Vergangenheit häufig von Art. 352 AEUV Gebrauch gemacht (ex-Art. 305 EGV), der das Tätigwerden der Union auf Vorschlag der Kommission und nach Zustimmung des Rates auch in Politikbereichen möglich macht, obwohl in den Verträgen die hierfür erforderlichen Befugnisse nicht vorgesehen sind. Dafür muss dies erforderlich sein, um eines der Ziele der Verträge zu verwirklichen (siehe auch Schmidt-Preuß, 2010, S. 69).



Eigentümer/Betreiber für den Schutz der Kritischen Infrastrukturen verantwortlich (Erwägungsgrund 6), dennoch geht Schmidt-Preuß (2010, S. 71 f) davon aus, dass die Richtlinie eine Eigendynamik entwickeln wird. Grund hierfür ist die Verpflichtung der Mitgliedsstaaten, beispielsweise Sicherheitspläne (Art. 5) und Bedrohungsanalysen (Art. 7) für KRITIS zu erstellen und einen Sicherheitsbeauftragten zu benennen (Art. 6). Zwar ist damit zu rechnen, dass bis 2011, wenn die Maßnahmen umgesetzt sein müssen, weitere Entwicklungen hinzukommen, jedoch fehlt es an Handlungsempfehlungen und praktischen Umsetzungsmöglichkeiten für die Mitgliedsstaaten.

Auf nationaler Ebene ist die Zuständigkeit zur Regelung von Infrastrukturen zwischen Bund, Ländern und Kommunen verteilt (Stober, 2010, S. 123 f). Die Analyse der unterschiedlichen normativen Regelungsmöglichkeiten auf den verschiedenen Ebenen, kann hier nicht vorgenommen werden. Handlungsmöglichkeiten müssten jedoch überprüft werden.

Letztendlich bleibt jedoch das grundsätzliche Problem bestehen, dass eine systematische Planung zur Reduktion der Anfälligkeit den Zielen der freien Marktwirtschaft wiedersprechen kann, wobei die Herstellung eines Gleichgewichts zwischen Energiepreisen und Versorgungssicherheit eine Herausforderung ist. Hier müssen neue Lösungsansätze entwickelt werden, an deren Gestaltung sowohl Betreiber, als auch Staat und Verbraucher teilhaben sollten (IRGC, 2006, S. 51). Eine Umsetzungsmöglichkeit bieten dabei Public Private Partnerships (PPPs), die auch im Rahmen des Kapitels *Risk Governance* (Kapitel 6.4) erläutert werden.

**Liberalisierung**

Zwar wurde durch die Marktliberalisierung auf der einen Seite die Anfälligkeit des Systems durch Zunahme der Anzahl der Akteure und die Umnutzung der Stromnetze erhöht, andererseits haben sich so auch neue Möglichkeiten ergeben. Beispielsweise selbstregulative Maßnahmen, die auf europäischer Ebene eine Rolle spielen. Hier wurde durch die UCTE die Möglichkeit geschaffen, Strommengen in Sekundenschnelle grenzüberschreitend im europäischen Verbundnetz zur Verfügung zu stellen (Schmidt-Preuß, 2010). Diese Errungenschaft brachte jedoch, wie in Kapitel 4.2 beschrieben, auch die Fragmentierung des Marktes in eine Vielzahl von Akteuren mit sich, zwischen denen eine enge Kooperation, insbesondere in Notfallsituationen notwendig ist. Hierfür ist die Bereitstellung von Echtzeit-Daten unerlässlich, um geeignete Maßnahmen ergreifen zu können (De Vries et al., 2006, S. 78). Ferner stellt sich in diesem Zusammenhang die Frage, wie die Kooperation gefördert, Ziele entwickelt und bestimmte Sicherheitsstandards erreicht werden können, zumal die Vielzahl der Akteure dies schwierig macht. Eine Möglichkeit stellt dabei der Risk Governenance Ansatz dar, der in Kapitel 6.4 gesondert vorgestellt wird.



### 6.2.2 Systemische Faktoren

Ein Hauptpunkt der systemischen Faktoren, der die Elektrizitätsversorgung anfällig macht, ist die Komplexität des Systems, die nur unzureichend erfasst ist. Hier bedarf es weiterer Forschung, die sowohl die Modellierung des Systems, als auch die systematische Erfassung und Auswertung von Ausfällen beinhaltet (IRGC, 2006, S. 27). Eine systematische Betrachtung der Ereignisse der Vergangenheit kann insbesondere zu einer Priorisierung der zu ergreifenden Maßnahmen führen.

Eine Möglichkeit mit dem Problem der Abhängigkeit der Elektrizitätsversorgung, beispielsweise von IT-Inputs oder Rohstoffen umzugehen, stellt die Reduktion der Abhängigkeit und damit die Schaffung von Autarkie der KRITIS dar. Allerdings ist dies nur bedingt mit vertretbarem Aufwand möglich (Lenz, 2009, S. 54). Die Dezentral-isiserung des Systems, beispielsweise durch erneuerbare Energien ist dabei jedoch eine Entwicklungsmöglichkeit in diese Richtung.

Wie in Kapitel 4.2 beschrieben, setzt sich die Komplexität der Elektrizitätsversorgung jedoch nicht nur aus technischen Komponenten, sondern auch aus der Vielzahl der Akteure zusammen. Um diesem Aspekt gerecht zu werden und sicherzustellen, dass sämtliche Betroffene in den Prozess zur Reduktion der Verwundbarkeit einbezogen werden, müssen *Risk Governance* Ansätze berücksichtigt werden (siehe auch 6.4) (Kröger, 2008, S. 1786). Eine besondere Herausforderung liegt hierbei in der grenzüberschreitenden Natur der Komplexität, die zwangsläufig auch internationale Koordination, zumindest auf europäischer Ebene, erfordert.

### 6.2.3 Technologische Faktoren

Im Rahmen der Analyse der Anfälligkeit der Elektrizitätsversorgung wurde in Kapitel 4.2 zunächst auf die Qualität der einzelnen Komponenten hingewiesen. Diese müssen zunächst den Anforderungen entsprechen und anschließend kontinuierlich gewartet, gepflegt und erneuert werden (Lenz, 2009, S. 56 f; IRGC, 2006, S. 27). Fraglich ist an dieser Stelle, ob diese Maßnahmen von den Betreibern den Ansprüchen genügend umgesetzt werden. Hier bedarf es rechtsverbindlicher Regeln innerhalb des gesamten Versorgungsnetzes, die kontrolliert und durchgesetzt werden können (De Vries et al., 2006, S. 82 f), wozu auch Strafen für deren Nichterfüllung gehören (Masera et al., 2006a, S. 103).

Im Rahmen der technischen Faktoren wurde das (n-1)-Kriterium und seine Bedeutung für das Elektrizitätssystem im liberalisierten, gewachsenen Markt thematisiert. Die Festlegung angemessener Sicherheitsziele und Maßnahmen zur Erlangung derselben beschränken sich derzeit jedoch zumeist auf diesen einfachen Sicherheitsstandard. Für komplexe Systeme, wie das der Elektrizitätsversorgung in Europa, sind jedoch



anspruchsvollere Maßnahmen notwendig. Der Austausch von Echtzeit-Daten könnte hier ein erster Ansatzpunkt sein (IRGC, 2006, S. 49) und wurde bereits im Nachgang an den Stromausfall im Emsland von der Bundesnetzagentur (2007) empfohlen, insbesondere, um das Zusammenwirken zwischen den Betreibern, aber auch der unterschiedlich flexiblen Erzeugungsarten wie Wind und Atomstrom zu koordinieren. Kapitel 6.3.3 geht darauf ein, welche Möglichkeiten im Rahmen der Dezentralisierung und dem Einsatz erneuerbarer Energien bestehen, mit fluktuierender Stromproduktion umzugehen.

Im Zusammenhang mit IT-Infrastrukturen, auf die das Elektrizitätssystem angewiesen ist, und die selber Auslöser von Fehlern sein können, müssen die Unternehmen aber auch gesonderte Strategien entwickeln, wobei angemessene Technologien und Standards Verwendung finden sollten. Bei der Enwicklung geeigneter Strategien sollte dabei berücksichtigt werden, dass diese KRITIS eine Schlüsselfunktion für eine funktionierende Stromversorgung hat (Masera et al., 2006, S. 116).

### 6.2.4 Menschliche Faktoren

In der Analyse der Anfälligkeit wurden die beiden Hauptaspekte des menschlichen Versagens im Bereich der *regelbasierten* und *wissensbasierten Fehler* festgestellt. Hier gibt es Handlungsbedarf im Bereich der Abstimmung zwischen den Betreibern der Elektrizitätsinfrastruktur bezüglich einheitlicher Regeln in Notfallsituationen. Im Zusammenhang mit möglichen Kaskadeneffekten können umfangreiche Wiederherstellungsmaßnahmen erforderlich sein. Diese sind auf entsprechende Informations- und Kommunikationstechnologien und -funktionen ebenso angewiesen, wie auf menschliche Faktoren, wie beispielsweise eine entsprechende Schulung (Gheorge et al., 2006, S. XVII). Hier muss der Zugang zu Echtzeit-Daten für die Mitarbeiter in Kombination mit Schulungen für ihre Handhabung verbessert werden, damit auf dieser Basis Entscheidungen getroffen werden können. Auch szenarien-basierte Trainings können im Umgang mit Zwischenfällen helfen, Fehler zu reduzieren (IRGC, 2006, S. 28).



## 6.3 Bewältigungskapazität

Auf europäischer Ebene wird eine Strategie verfolgt, die im Zuge der Bewältigungskapazität einerseits Prävention in Form von *„Risiko- und Bedrohungsanalysen im Bereich Kritischer Infrastrukturen, erhöhte Sicherheitsvorkehrungen, Förderung gemeinsamer Sicherheitsstandards und des Erfahrungsaustausches sowie der Koordination und Zusammenarbeit“* (EU-Kommission, 2005, S. 4) betreibt. Andererseits soll die Behebung der Folgen (*Reaktion*) von Anschlägen und Katastrophen durch den *„Austausch von Fachkenntnissen und Erfahrungen, Ausarbeitung von Szenarien, Ausbildungsmaßnahmen, Schaffung eines funktionierenden Krisenmanagements [und durch] [...] Frühwarnsystemen [sowie] Zivilschutzmaßnahmen“* (EU-Kommission, 2005, S. 4) einen weiteren Schwerpunkt bilden.

### 6.3.1 Prävention

Im Rahmen der Prävention können insbesondere die in Abschnitt 4.3 genannten technischen Maßnahmen zur Verbesserung der Bewältigungskapazität verstärkt werden. Hierzu gehören Redundanzen, die die Funktion einer anderen Komponente übernehmen können, wenn diese ausfällt. Auch Back-ups, insbesondere in öffentlichen Einrichtungen, die auf die Aufrechterhaltung der Versorgung auch während eines Stromausfalls dringend angewiesen sind, wie beispielsweise Krankenhäuser, spielen eine wichtige Rolle.

### 6.3.2 Reaktion

Die Bewältigungskapazität im Rahmen der Reaktion wird durch den Wiederherstellungsaufwand und Grad der Vorbereitung auf ein solches Ereignis beeinflusst. Hier sollten die technischen Möglichkeiten ausgenutzt werden, die den Wiederherstellungsaufwand einer Komponente oder eines Prozesses nach einem Stromausfall erleichtern können (Lenz, 2009, S. 60).

Im Rahmen der Vorbereitung auf einen Stromausfall kann der Einsatz durch Notfallübungen geübt und so ein reibungsloserer Ablauf im Ereignisfall gewährleistet werden. Ein Beispiel für die Durchführung von Notfallübungen im Bereich des nationalen Krisenmanagements stellt die Länder Übergreifende Krisenmanagement-Übung/Exercise (LÜKEX) dar. Während der Durchführungsphase sind bis zu 3.000 Personen aus unterschiedlichen Krisenstäben in die Übung involviert. Bisher wurden seit 2004 alle zwei Jahre ressort- und bundesländerübergreifend vier LÜKEX-Übungen[32] mit dem Ziel durchgeführt, die Übungskultur im Bereich des Krisen-

[32] LÜKEX 04: Stromausfall, Terroranschlag; LÜKEX 05: WM 2006; LÜKEX 07: Pandemie; LÜKEX 09/10: Schmutzige Bombe; LÜKEX 11: IT-Sicherheit (in Planung) (BBK, 2010b)



managements weiterzuentwickeln und somit voranzutreiben. Ergebnis dieser Übungen ist ein Bericht, welcher Handlungsempfehlungen für das strategische Krisenmanagement bereitstellt. Außerdem fließen die Erkenntnisse auch in die Forschung im Bevölkerungsschutz, die Weiterentwicklung technischer Führungs- und Einsatzmittel, sowie in die Aus- und Weiterbildung von Personal ein. LÜKEX dient folglich auch dem Austausch bzw. der Kooperation zwischen Krisen- bzw. Verwaltungsstäben von Bund und Ländern, privaten Betreibern Kritischer Infrastrukturen, Hilfsorganisationen sowie Verbänden, da sie sich gemeinsam auf länger anhaltende komplexe Krisenlagen durch die Übungen vorbereiten (BBK, 2010b). Besonders bei der Umsetzung dieser Vorhaben ist eine effektive und kooperative Partnerschaft zwischen Staat und Betreibern der Infrastrukturen von enormer Bedeutung. Daher ist eine Stärkung der Zusammenarbeit von Bund und Ländern, sowie eine Kooperation auf europäischer Ebene notwendig (Schäuble, 2010, S. 24).

Des Weiteren könnte die Einrichtung eines Warn- und Informationsnetzes für Kritische Infrastrukturen, vorgeschlagen von der EU-Kommission, die Informationslage und damit die Entscheidungsgrundlage für die Betreiber verbessern (Kloepfer, 2010). Das Critical Infrastructure Warning Information Network (CIWIN) ist Teil der EU-Strategie ein horizontales und sektorübergreifendes System zum Schutz Kritischer Infrastrukturen aufzubauen.[33] Primäres Ziel des Netzwerks soll es sein, ein Informationssystem zu errichten, das *„zur Förderung der Integration und besseren Koordinierung der unabhängig voneinander durchgeführten nationalen Forschungsprogramme im Bereich des Schutzes Kritischer Infrastrukturen beiträgt und das es den Mitgliedstaaten und der Kommission ermöglicht, Informationen und Warnmeldungen, die den Schutz Kritischer Infrastrukturen betreffen, auszutauschen und ihren Dialog in diesem Bereich zu intensivieren*“ (Kommission, 2008, S. 11).

### 6.3.3 Möglichkeiten durch erneuerbare Energien

Wie schon in Kapitel 2 aufgezeigt wurde, wird die Stromversorgung noch weitestgehend durch fossile Brennstoffe sowie durch die Kernenergie gewährleistet. Nichtsdestotrotz gewinnen erneuerbare Energien immer weiter an Bedeutung, um der Rohstoffknappheit, dem Klimawandel, der weiteren Abhängigkeit der Atomenergie und den Energieimporten entgegenzuwirken. Dies wurde darin manifestiert, dass sich die Europäische Union zum Ziel gesetzt hat, 20% der Endenergie bis zum Jahr 2020 aus erneuerbaren Ressourcen zu erwirtschaften. Die Bundesregierung hat dabei bezüglich des Elektrizitätssektors beschlossen – und dies auch im Erneuerbaren-Energien-Gesetz (EEG) verankert – bis zum Jahr 2020 30% des Stroms aus regenerativen Energiequellen zu gewinnen (Haber & Bliem, 2010, S. 2; Schwarz et al., 2008, S. 1; Bundestag, 2010).

[33] Beispielsweise legte die Kommission mit KOM(2008) 676 endgültig dem Rat einen Vorschlag über ein Warn- und Informationsnetz für kritische Infrastrukturen (CIWIN) vor.



Wie aus Abbildung 30 ersichtlich wird, ist bei der Bruttostromerzeugung in der Zeitspanne von 1990 bis 2008 ein Anstieg von 15,9% zu verzeichnen, wobei der Abfall der Bruttostromerzeugung um 6,3% im Jahr 2009 mit der Wirtschaftskrise zu erklären ist. Wie man weiter erkennen kann, stellen die fossilen Energieträger im Jahr 2009 mit einem Anteil von ca. 60% immer noch die zentralen Energieträger für die Stromversorgung dar (Bräuninger et al., 2010, S. 8 f).

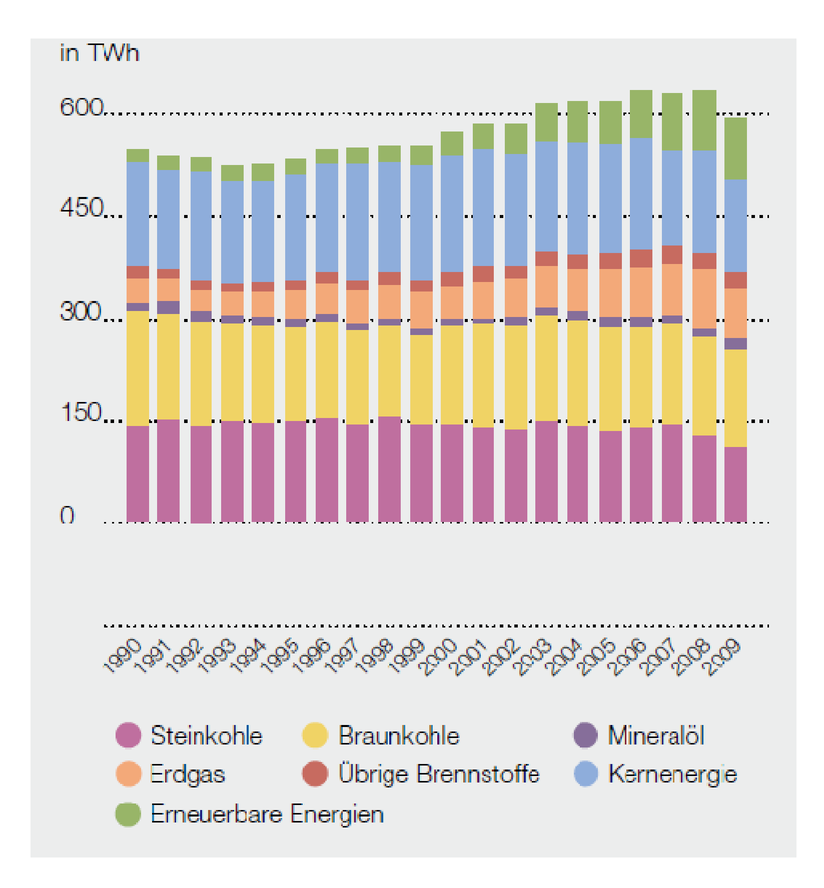



**Abbildung 30: Bruttostromerzeugung nach Energieträgern in Deutschland**

Quelle: (Bräuninger et al., 2010, S. 8)

Dennoch hat sich der Anteil der erneuerbaren Energien an der Bruttostromerzeugung seit 1990 deutlich erhöht. Dies hängt auch damit zusammen, dass laut des Erneuerbaren-Energien-Gesetzes (EEG) *„die Netzbetreiber dazu verpflichtet [sind], Anlagen zur Erzeugung von Strom aus erneuerbaren Energien und aus Grubengas unverzüglich vorrangig an der Stelle an ihr Netz anzuschließen (Verknüpfungspunkt), die im Hinblick auf die Spannungsebene dazu geeignet ist, und die in der Luftlinie die kürzeste Entfernung zum Standort der Anlage aufweist, wenn nicht ein anderes Netz einen technisch und wirtschaftlich günstigeren Verknüpfungspunkt bietet (§5 Abs. 1 Satz 1 EEG)“* ((Haber & Bliem, 2010, S. 2) zitiert nach (Bundestag Deutschland, 2010)). Im



Jahr 2009 lag somit der Anteil der erneuerbaren Energien an der Bruttostromerzeugung bei einem Wert von 15,6% (Bräuninger et al., 2010, S. 8).

Die Windkraft hat dabei erheblich zum Wachstum der Stromerzeugung aus erneuerbaren Energien beigetragen. Sie hat seit Mitte der 1990er Jahre ein kontinuierliches Wachstum zu verzeichnen und bestreitet nun einen Anteil von etwa 6,3% an der Bruttostromerzeugung und einen Anteil von 40,7% an der Stromerzeugung aus erneuerbaren Energien (siehe Abbildung 31). Die Windkraft hat seit 2006 somit die Wasserkraft überholt, welche bis dahin die bedeutendste erneuerbare Energiequelle für die Energieerzeugung darstellte. Dennoch darf nicht übersehen werden, dass der Wasserkraft eine große Bedeutung zugeschrieben wird, was daraus resultiert, dass sie zusammen mit der Biomasse[34] als einzige erneuerbare Energiequelle eine sogenannte Grundlastfähigkeit besitzt. Dies bedeutet, dass bei der Wasserkraft, sowie bei der Stromerzeugung aus Biomasse keine Abhängigkeit vom Wettergeschehen existiert, sondern konstant Strom gewonnen werden kann. Dies ist vor allem deswegen von großer Bedeutung, da Strom schlecht gespeichert werden kann und daher direkt nach der Erzeugung zum Verbraucher transportiert werden muss. Schließlich sind Wasserkraftwerke bei der Stromerzeugung für Spitzenlastzeiten prädestiniert, da sie über sogenannte Schnellstartfähigkeiten verfügen (Bräuninger et al., 2010, S. 8 f).

[34] Zur Biomasse werden biogene Festbrennstoffe, biogene flüssige Brennstoffe, Biogas, Klärgas, Deponiegas sowie biogener Anteil des Abfalls gezählt (siehe Abbildung 31).



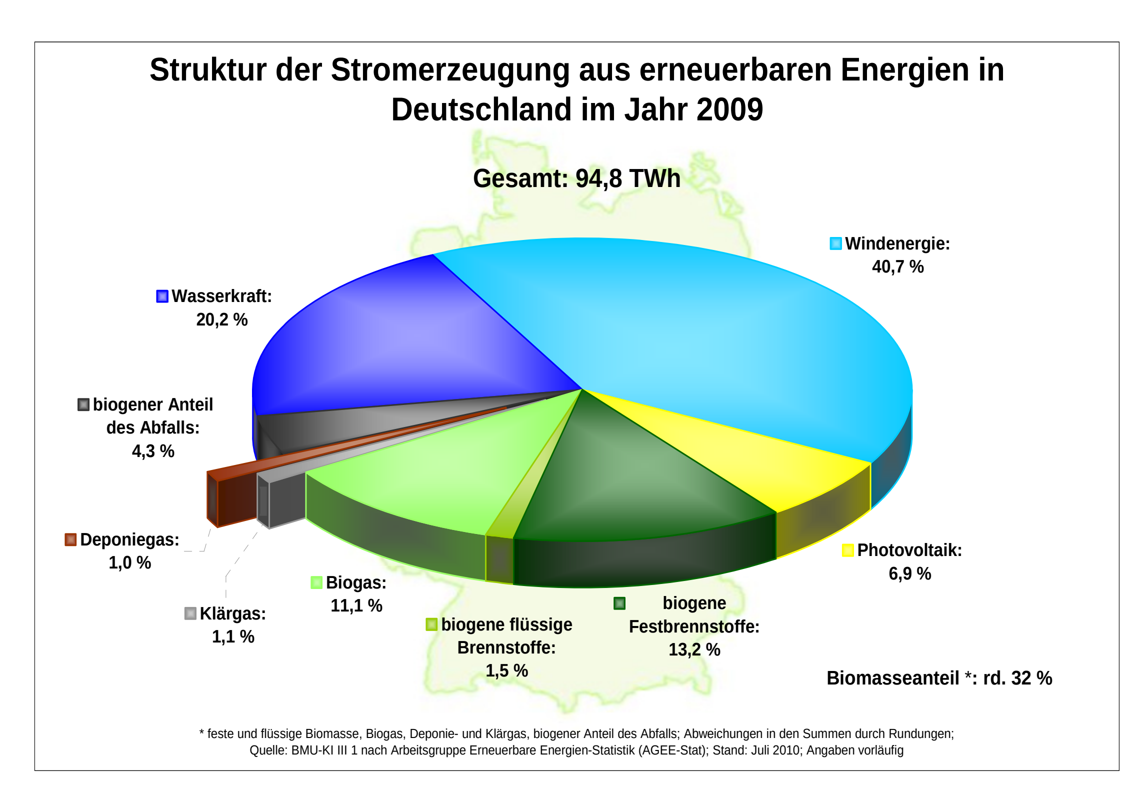



**Abbildung 31: Struktur der Stromerzeugung aus erneuerbaren Energien in Deutschland im Jahr 2009**

Quelle: (Ottmüller & Nieder, 2010, S. 9)

Im Umkehrschluss muss festgestellt werden, dass durch die erneuerbaren Energien wie beispielsweise Windkraft oder Photovoltaikanlagen neue Herausforderungen aufkommen, da diese über keine Grundlastfähigkeit verfügen. Vielmehr ist die Stromgewinnung dieser erneuerbaren Energien vom Wettergeschehen abhängig, wodurch Leistungsschwankungen bei der Stromerzeugung entstehen. Zum jetzigen Zeitpunkt werden diese Leistungsschwankungen noch von Großkraftwerken mit Grundlastfähigkeit, die aus fossilen oder atomaren Energiequellen gespeist werden, aufgefangen. In diesem Zusammenhang wird auch von Brückentechnologien gesprochen, welche die Netze solange unterstützen, bis die Stromversorgung ausschließlich aus erneuerbaren Energien erfolgen kann. Somit wird mit Hochdruck an neuen Technologien geforscht, um mit den Leistungsschwankungen der erneuerbaren Energien umzugehen – mit dem Ziel nicht mehr auf Großkraftwerke angewiesen zu sein. In diesem Zusammenhang soll das Konzept des sogenannten Smart Grids vorgestellt werden (Schmidt & Vohrer, 2010, S. 4 f).

Das Smart Grid stellt *„ein intelligentes Stromnetz [dar], das die Verhaltensweisen und Handlungen aller Nutzer, die an dieses Netz angeschlossen sind (also Erzeuger und Verbraucher ebenso wie Akteure, die beides sind, also sowohl Stromerzeuger als auch Stromverbraucher) miteinander vernetzen kann, um eine nachhaltige, wirtschaftliche*



*effiziente und sichere Stromversorgung zu ermöglichen"* (Gorelova, 2010, S. 3). Smart Grids unterscheiden sich somit vom bisherigen Stromnetz in der Hinsicht, dass nicht mehr verbrauchsorientiert Strom erzeugt wird, sondern ein erzeugungsorientierter Verbrauch angestrebt wird. Folglich besteht die Möglichkeit, mit den enormen Schwankungen und der Unvorhersehbarkeit der erneuerbaren Energien umzugehen (BMWi, 2010, S. 5; Hammons, 2008, S. 470 ff).

Wie man in Abbildung 32 erkennen kann, ist in das Smart Grid die sogenannte Informations- und Kommunikationstechnik (IKT) integriert, durch die unterschiedliche Akteure digital miteinander vernetzt sind. So können Kunden über das Internet durch sogenannte Smart Meter – also digitale Strommessgeräte welche in den Häusern beziehungsweise Wohnungen installiert sind – ihren Stromverbrauch genau einsehen und erkennen, zu welcher Zeit der Strom wie viel kostet (Real-time-Preise). Das Ziel besteht darin, durch Preisregulierungen für die Verbraucher Anreize zu schaffen, mehr oder weniger Strom zu verbrauchen. Denn in Zeiträumen mit einem Stromüberschuss – beispielsweise ausgelöst durch Starkwinde – ist der Strom günstiger als in Zeitperioden, in denen, beispielsweise ausgelöst durch Windflauten, weniger Strom gewonnen werden kann. So kann beim Kunden der Anreiz geschaffen werden, die Wasch- oder Spülmaschine in einem Zeitraum mit höherem Stromvorkommen zu benutzen. Die Smart Meter[35] geben auch gleichzeitig die notwendigen Informationen über den Stromverbrauch der Verbraucher an das Gesamtnetz weiter, sodass die Erzeugung, die Netzbelastung sowie der Verbrauch ideal aufeinander abgestimmt werden können (BMWi, 2010, S. 5 ff; Gorelova, 2010, S. 4 ff; Wissner, 2010, S. 5 f; Schmid, et al., 2005, S. 17 ff).

Auch können sich die Verbraucher durch eigene Photovoltaik- oder Windkraftanlagen an der Stromerzeugung beteiligen und der von ihnen gewonnene Strom wird in das Stromnetz eingespeist. Sie können somit aktiv in das Stromnetz eingreifen. Eine große Rolle wird dabei auch der e-Mobility-Branche[36] zugeschrieben, wobei die Batterien von Elektroautos zum einen bei Bedarf durch das Stromnetz aufgeladen werden, gleichzeitig jedoch auch bei Nicht-Gebrauch den Strom zurück in das Netz einspeisen können. Somit tragen die Elektroautos auch dazu bei, dass in Spitzenverbrauchszeiten genügend Strom im Netz vorhanden ist und Stromengpässe vermieden werden(Gorelova, 2010, S. 7 ff; BMWi, 2010, S. 6 ff; Horbaty & Rigassi, 2007, S. 3 ff).

[35] Die Smart Meter können dabei den Verbrauch der stromverbrauchenden Geräte messen, da alle Geräte durch die sogenannte Plug & Play Funktion mit dem Regelsystem verbunden sind.
[36] Die deutsche Übersetzung lautet Elektroauto-Branche.



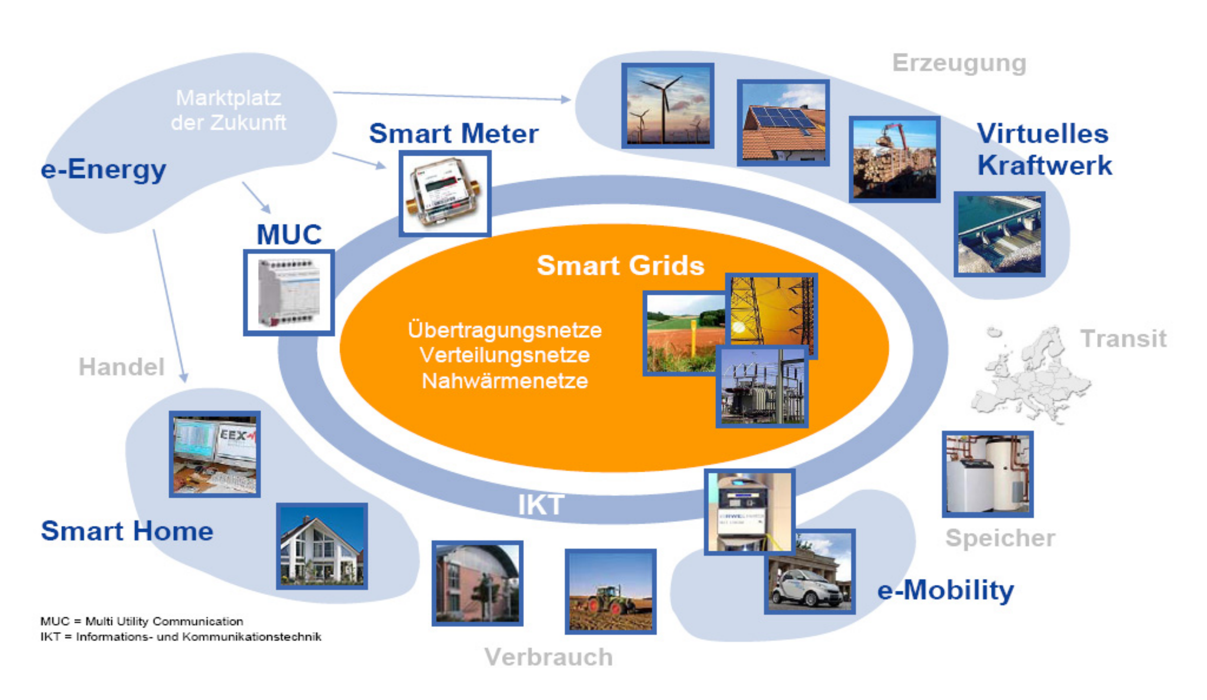



**Abbildung 32: Smart Grids**

Quelle: ((Haber & Bliem, 2010, S. 2) zitiert nach (BDEW, 2009 S. 5))

Insgesamt zeichnet sich das Konzept der Smart Grids durch eine äußerst starke Vernetzung der einzelnen Akteure aus, wodurch gewährleistet werden soll, dass die Stromgewinnung aus erneuerbaren Energien ideal mit den Ansprüchen der Verbraucher abgestimmt wird. Während das herkömmlich zentral gesteuerte System der Stromwirtschaft durch die Bereitstellung von Erzeugungskapazitäten sowie dem Handel von Energie als effizient bezeichnet werden kann, gilt dieses jedoch – wie anhand der Stromausfälle in 4.1.3 gezeigt wurde – gegenüber Störungen als verwundbar. Durch Smart Grids wird das Stromnetz wie in Abbildung 33 dargestellt, über ein großes Portfolio unterschiedlicher erneuerbarer Energieanlagen versorgt, sodass dadurch die bereits heutzutage schon hohe Versorgungssicherheit noch weiter ausgebaut werden kann. So kann durch Smart Grids mit ihrer dezentralen Struktur auch die Anfälligkeit gegenüber Störungen herabgesetzt werden. Zum einen hängt dies damit zusammen, dass durch die vielen unterschiedlichen Energiequellen Störungen einer Energieressource durch eine andere Stromerzeugungsanlage kompensiert werden kann. Zum anderen können die Verbraucher aktiv in das Stromnetz eingreifen und dadurch positiv daran mitwirken, dass es nicht zu Engpässen in der Stromversorgung kommt (Haber & Bliem, 2010, S. 3). Wie jedoch bereits in Kapitel 0 erläutert wurde, birgt die neue Technologie der Smart Grids auch Gefahren gegenüber Cyberattacken und Datenmissbrauch. Es ist daher von großer Bedeutung, Maßnahmen zur Verringerung der Sicherheitsrisiken zu entwickeln (siehe dazu Kapitel 0). (McDaniel & McLaughlin, 2009)



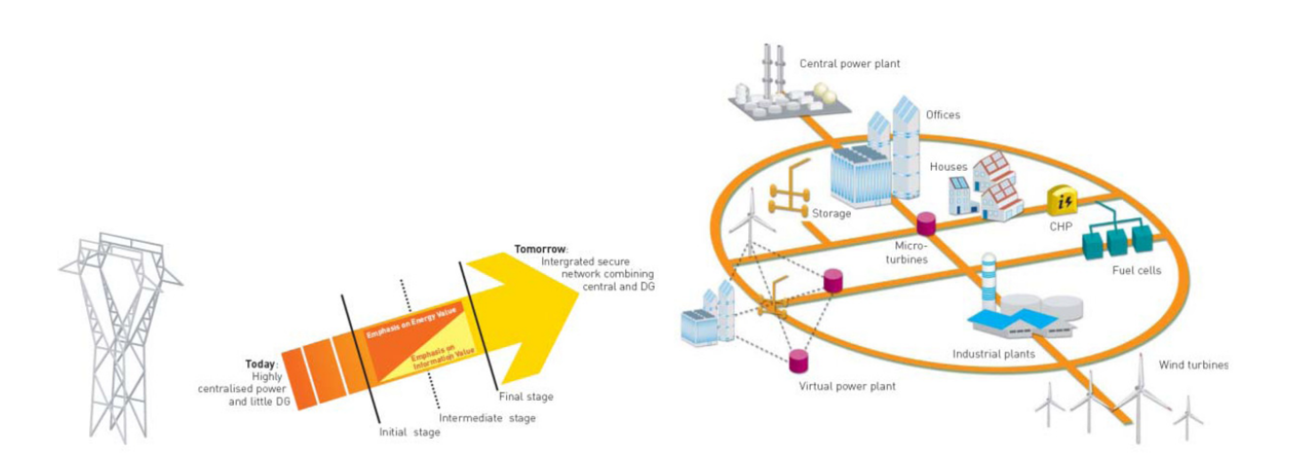



**Abbildung 33: Von der heutigen, zentralisierten Stromversorgung zu einem vernetzten Stromnetz mit zentralen und dezentralen Produktionsanlagen**

Quelle: ((Horbaty & Rigassi, 2007, S. 7) zitiert nach (European Commission, 2006, S. 18))

Abschließend kann also festgehalten werden, dass die Smart Grids die Bewältigunskapazität erhöhen könnten. Ihr Ausbau und die Einführung zugehöriger Technologien, wie beispielsweise Smart Meter, werden von der Bundesregierung gezielt gefördert[37]. Jedoch können auch Probleme beziehungsweise mögliche Rückschläge im Voranschreiten der Einführung der erneuerbaren Energien mit ihren Technologien gesehen werden. Dazu zählt auch der Plan der Bundesregierung, die Laufzeit der Atomkraftwerke gegenüber den Plänen aus dem Jahr 2002, die einen Ausstieg aus der Atomenergie bis etwa zum Jahr 2021 vorsahen, um durchschnittlich 12 Jahre zu verlängern. Zwar kann die Stromversorgung nicht ab sofort ausschließlich durch die erneuerbaren Energien abgedeckt werden, sodass die Brückentechnologien weiter eine Rolle spielen müssen, um Spitzenlasten aufzufangen. Allerdings müssen diese auch flexibel gestartet werden können (Schnellstart wie beispielsweise bei Gasturbinenwerken), um auf die Leistungsschwankungen der erneuerbaren Energien reagieren zu können. Atomkraftwerke sind dabei eher ungeeignet, da sie eine recht lange Zeitspanne benötigen, um hoch- und runtergefahren zu werden. „*Atomkraftwerke sind die unflexibelsten Anlagen im traditionellen Kraftwerkspark. Denn AKWs sind kaum regelbar und häufiges An- und Abschalten wird schon aus Sicherheitsgründen soweit irgend möglich vermieden. Durch eine Laufzeitverlängerung entstünde aufgrund der geringen Flexibilität der Anlagen ein Druck, die Stromversorgungskapazitäten auch möglichst vollständig am Markt abzusetzen*“ (Fischedick, Supersberger, & Zeiss, 2009,

[37] Durch das Energiewirtschaftsgesetz ist seit 1. Januar 2010 vorgeschrieben, dass deutschlandweit in alle Neubauten sowie Sanierungsprojekte intelligente Stromzähler (Smart Meters) eingebaut werden müssen, durch welche der tatsächliche Stromverbrauch abgelesen werden kann. Außerdem soll es bis zum Jahresende 2010 möglich sein, dass die Stromanbieter den Verbrauchern variable Stromtarife anbieten können(Gorelova, 2010, S. 11).



S. 7). Somit würden auch die Anreize verloren gehen die Stromversorgung aus erneuerbaren Energien weiter voranzutreiben und die Entwicklung energieeffizienterer Technologien würde sich verzögern (Schmidt & Vohrer, 2010, S. 7 ff; Fischedick et al., 2009, S. 7 ff; focus-online, 2010).

## 6.4 Risk Governance

Als ein wichtiger Aspekt zur Reduktion der Verwundbarkeit ist deutlich geworden, dass an diesem Prozess viele verschiedene Akteure beteiligt werden müssen. Handlungsmöglichkeiten sollten daher an ein Governance Konzept angelehnt werden. Dieses beschreibt beispielsweise Renn (2009) wie folgt:

> *„[...] It involves the four central actors in modern plural societies: governments, economic players, scientists and civil society organizations"*

Sinngemäß soll *Governance* die vier zentralen Akteure der modernen pluralistischen Gesellschaften (Regierungen, wirtschaftliche Akteure, Wissenschaftler und Zivilgesellschaft) in den Entscheidungsfindungsprozess einbinden.

Bezüglich des Risikos muss verdeutlicht werden, dass der Begriff in verschiedenen Communities und auch innerhalb dieser unterschiedlich definiert und vielschichtig verwendet wird. Gemäß der im Rahmen dieser Studie verwendeten Definitionen und Konzepte (siehe Kapitel 3.2) handelt es sich bei dem Begriff Risiko um die Kombination der Wahrscheinlichkeit des Auftretens einer Gefahr und ihrer negativen Auswirkungen (UN/ISDR, 2009). Da die negativen Auswirkungen durch die Verwundbarkeit des Systems bestimmt werden, beschreibt eine Erweiterung der Definition um die Wahrscheinlichkeit des Eintretens einer bestimmten Gefahr ein bestehendes Risiko.

Um die Vielzahl der betroffenen Akteure, wie beispielsweise Regierung, Betreiber und schließlich Verbraucher in den Prozess der Risko- und damit der Verwundbarkeitsreduktion einzubinden, ist ein ganzheitlicher Ansatz wichtig, um den unterschiedlichen Faktoren, die die Anfälligkeit der KRITIS beeinflussen, gerecht werden zu können (Kröger, 2008).[38] Die nähere Betrachtung möglicher *Risk Governance* Ansätze ist auch deswegen sinnvoll, weil durch die Komplexität der Elektrizitätsversorgung und die vielfältigen Abhängigkeiten anderer KRITIS viele Ursache-Wirkungs-Gefüge noch unbekannt oder nicht hinreichend erforscht sind (siehe Kapitel 5.3). Dies führt dazu, dass Entscheidungsträger auch ohne umfangreiche Informationsgrundlage Entscheidungen treffen müssen (Renn, 2008, S. 7). In Anlehnung an Hohenemser et al.

[38] Aus diesem Grunde werden ausgewählte Risk Governance Ansätze trotz möglicher Divergenzen des Risikoverständnisses vorgestellt.



(1983) identifiziert der IRGC (2005), wie in Abbildung 34 dargestellt, daher zunächst am Beispiel der Atomenergie mögliche Interventionspunkte, an denen ein Risiko beeinflusst werden kann:

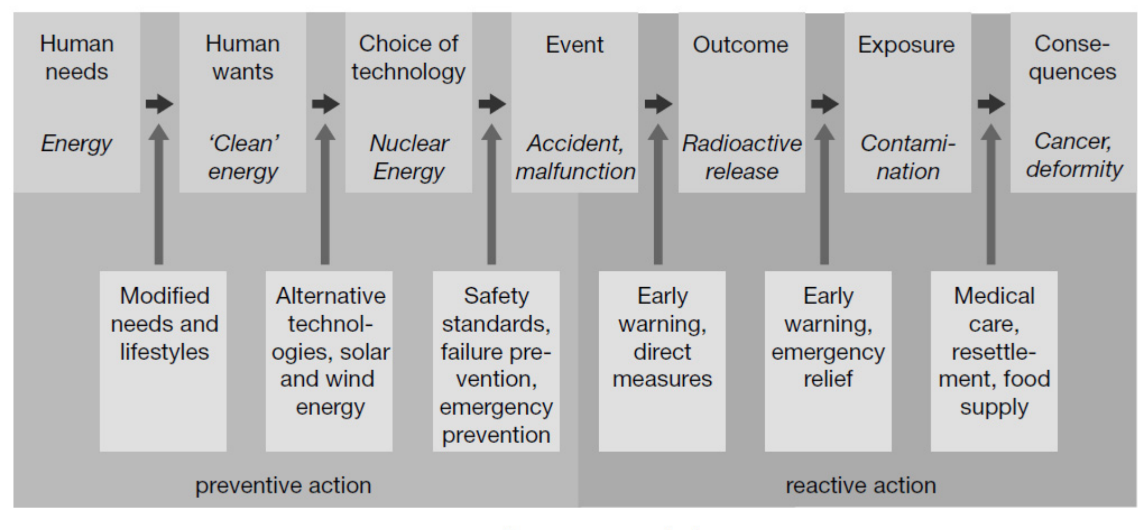



**Abbildung 34: Sieben Schritte einer Risiko-Kette: Das Beispiel Atomenergie**

Quelle: (IRGC, 2006, S. 21)

Innerhalb dieser verschiedenen Interventionspunkte existieren verschiedene Interventionsschritte, die in Abbildung 35 dargestellt sind. Dabei geht es in der ersten, der *Pre-Assessment* Phase darum, zunächst den Rahmen des Risikos zu identifizieren.

In der *Risk Appraisal* Phase wird dann eine Wissensbasis geschaffen, die sowohl das Risiko selbst näher identifiziert als auch Lösungsmöglichkeiten und deren Auswirkungen näher beschreibt. Dabei spielt nicht nur die Abschätzung der Verwundbarkeit eine Rolle, sondern insbesondere auch die Wahrnehmung des Risikos. In diesem Schritt ergibt sich die besondere Herausforderung mit Komplexität und Unsicherheit umzugehen. Da diese Faktoren nicht abschließend einzuordnen sind, ist es besonders wichtig, sowohl das Wissen aller Stakeholder einzubeziehen, als auch deren Fragen und Bedenken zu berücksichtigen und diese transparent zu machen. Der wohl schwierigste Schritt erfolgt mit der Entscheidung über das zu akzeptierende Risiko (*Tolerability and Acceptibility Judgement*). Hierbei wird jedoch vorausgesetzt, dass das Wissen aus der zweiten Phase noch ergänzt wird, um eine Abschätzung darüber treffen zu können, welches Risiko, bzw. welche möglichen negativen Auswirkungen akzeptierbar sind und wie das Risiko bis zu diesem akzeptierbaren Punkt reduziert werden kann. Im letzten Schritt, dem Risk Managment werden Handlungsmöglichkeiten umgesetzt und ausgewertet, um anschließend die Situation wieder neu einzuschätzen und den Erfolg zu analysieren. (IRGC, 2005, S. 13 f)



Management Sphere:
Decision on & Implementation of Actions

Assessment Sphere:
Generation of Knowledge

Pre-Assessment
• Problem Framing
• Early Warning
• Screening
• Determination of Scientific Conventions

Risk Management
Implementation
• Option Realisation
• Monitoring & Control
• Feedback from Risk Mgmt. Practice
Decision Making
• Option Identification & Generation
• Option Assessment
• Option Evaluation & Selection

Communication

Risk Appraisal
Risk Assessment
• Hazard Identification & Estimation
• Exposure & Vulnerability Assessment
• Risk Estimation
Concern Assessment
• Risk Perceptions
• Social Concerns
• Socio-Economic Impacts

Tolerability & Acceptability Judgement
Risk Evaluation
• Judging the Tolerability & Acceptability
• Need for Risk Reduction Measures
Risk Characterisation
• Risk Profile
• Judgement of the Seriousness of Risk
• Conclusions & Risk Reduction Options

**Abbildung 35: IRGC Risk Governance Framework**

Quelle: (IRGC, 2005, S. 13)

Im Rahmen des *Risk Managements* ergeben sich dabei Möglichkeiten, mit den Charakteristika des Risikos, wie beispielsweise Komplexität oder Unsicherheit über mögliche Folgen, umzugehen. Renn (2008) stellt dabei in Anlehnung an IRGC (2005) verschiedene Instrumente vor, die in Tabelle 6 dargestellt sind.



**Tabelle 6: Risikocharakteristika und ihre Auswirkungen auf das Risk Management**

| Charakter-istikum | Management-Strategie | Geeignete Instrumente | Geeignete Instrumente |
|---|---|---|---|
| **Komplexität** | Risiko-Information | Charakterisierung des verfügbaren Wissens: | Epistemischer Diskurs |
| | (Akteure und Wirkungsketten) | • Instrumente zum Erreichen eines Experten-Konsensus<br>o Delphi- oder Konsens-Konferenz<br>o Meta-Analyse<br>o Szenario-Konstruktion, etc.<br>• Einbeziehung der Ergebnisse in Routine-Arbeitsabläufe | |
| | Robustheits-Fokus | Verbesserung der Puffer-Kapazität durch: | |
| | (Risiko-absorbierendes System) | • Zusätzliche Sicherheits-Faktoren<br>• Redundanz und Diversität im Design der Sicherheits-Bauteile<br>• Verbesserung der Bewältigungskapazität<br>• Errichtung von hochverlässlichen Organisationen | |
| **Unsicherheit** | Vorsichts-basiert | Nutzung von Gefahrencharakteristika als Proxies für Risikoannahmen: | Reflektiver Diskurs |
| | (Akteure) | • Sicherheitsräume<br>• ALARA (as low as reasonably achievable) – so niedrig wie vernünftig erreichbar und ALARP (as low as reasonable practicable) – so niedrig wie vernünftig praktizierbar<br>• BACT (best available control technology) – beste verfügbare Kontrolltechnik, etc. | |
| | Resilienz-fokussiert | Verbesserung der Bewältigungskapazität gegenüber Überraschungen: | |
| | | • Diversität der Mittel, um die gewünschten Ziele zu erreichen<br>• Reduktion der Verwundbarkeit<br>• Zulassen flexibler Handlungsmöglichkeiten<br>• Vorbereitung zur Anpassung | |
| **Ambiguität** | Diskurs-basiert | Anwendung von Konfliktlösungsmethoden zum Erreichen eines Konsens oder Toleranz gegenüber der Bewertung des Risikos und der ausgewählten Managementoptionen: | Partizipatorischer Diskurs |
| | | • Integration der Stakeholderbeteiligung<br>• Schwerpunktsetzung auf Kommunikation und soziale Diskurse | |

Quelle: (eigene Darstellung in Anlehnung an (Renn, 2008, S. 182 f) nach (IRGC, 2005))



Bezogen auf unterschiedliche Auffassungen (Ambiguität) zum Umgang mit dem Risiko in verschiedenen epistemischen Gemeinschaften, basierend auf unterschiedlichem Wissen und verschiedenen Interessen und Zielvorstellungen, stellen Public Private Partnerships eine Alternative dar. Möglich wäre hier beispielsweise die Vorgabe von Standards und Normen durch den Staat, gekoppelt mit ihrer Kontrolle durch Dritte in Verbindung mit Versicherungen, um ihre Umsetzung abzusichern (Renn, 2008, S. 181 ff). Dies hat den Vorteil, dass die Unternehmen die Maßnahmen zur Erreichung der Zielvorgaben selber aussuchen können. Die Kopplung von Aufsicht durch Dritt-Parteien mit Marktmechanismen durch Versicherungen ist dabei ein hilfreiches Mittel zur Gewährleistung der Umsetzung. Aufgrund der grenzüberschreitenden Natur des Risikos werden jedoch auch konsens- und anreizbasierte Strategien vorgeschlagen (Renn, 2008, S. 184).
Im Rahmen möglicher PPPs hat die President's Commission on Critical Infrastructure Protection (PCCIP) (1997) aufgrund der Vielzahl der betroffenen Akteure, der Interessen privater und staatlicher sowie internationaler und lokaler Stakeholder ein gemeinsames Beitragssystem zwischen Betreibern, national und lokal politisch Verantwortlichen vorgeschlagen. So könnte beispielsweise Beratung und Frühwarnung finanziert werden. Ferner könnten Innovationen und deren Umsetzung, umfangreiche Störfallmeldungen und Übungen zum Umgang mit neuen Gefahrensituationen entwickelt werden. Dabei sollte das gemeinsame System insbesondere dem Wissenstransfer und der Entwicklung neuer Sicherheitsmaßnahmen dienen (PCCIP, 1997, S. 47 ff).

Grundlegend ist im *Governance Prozess* die Kommunikation während des gesamten Prozesses. Dabei sollte insbesondere während der ersten Phase und der Festlegung des akzeptierbaren Risikos der enge Austausch zwischen den Experten, beispielsweise Wissenschaftler, Politiker und technisches Personal, gewährleistet werden. Zweitens muss das Risiko nach außen, also an die Bevölkerung kommuniziert werden. Jedoch sind weite Teile der Bevölkerung nicht mit den Ansätzen der Riskoabschätzung vertraut und versuchen, ihre eigenen Ansichten zu vertreten. Dabei ist es von entscheidender Bedeutung, der Bevölkerung das bestehende Risiko verständlich zu machen, da hiervon die nötige Vorbereitung, bzw. der entsprechende Umgang mit Gefahrensituationen abhängt (Renn, 2008, S. 201 ff). Dass diese Kommunikation im Bereich der Elektrizitätsversorgung noch nicht richtig funktioniert hat, zeigt dabei das Verwundbarkeitsparadoxon (Kapitel 5.2).

Insgesamt muss berücksichtigt werden, dass im Rahmen der Elektrizitätsversorgung mehrere Ebenen existieren, die die Verwundbarkeit beeinflussen, wie Abbildung 36 zeigt:



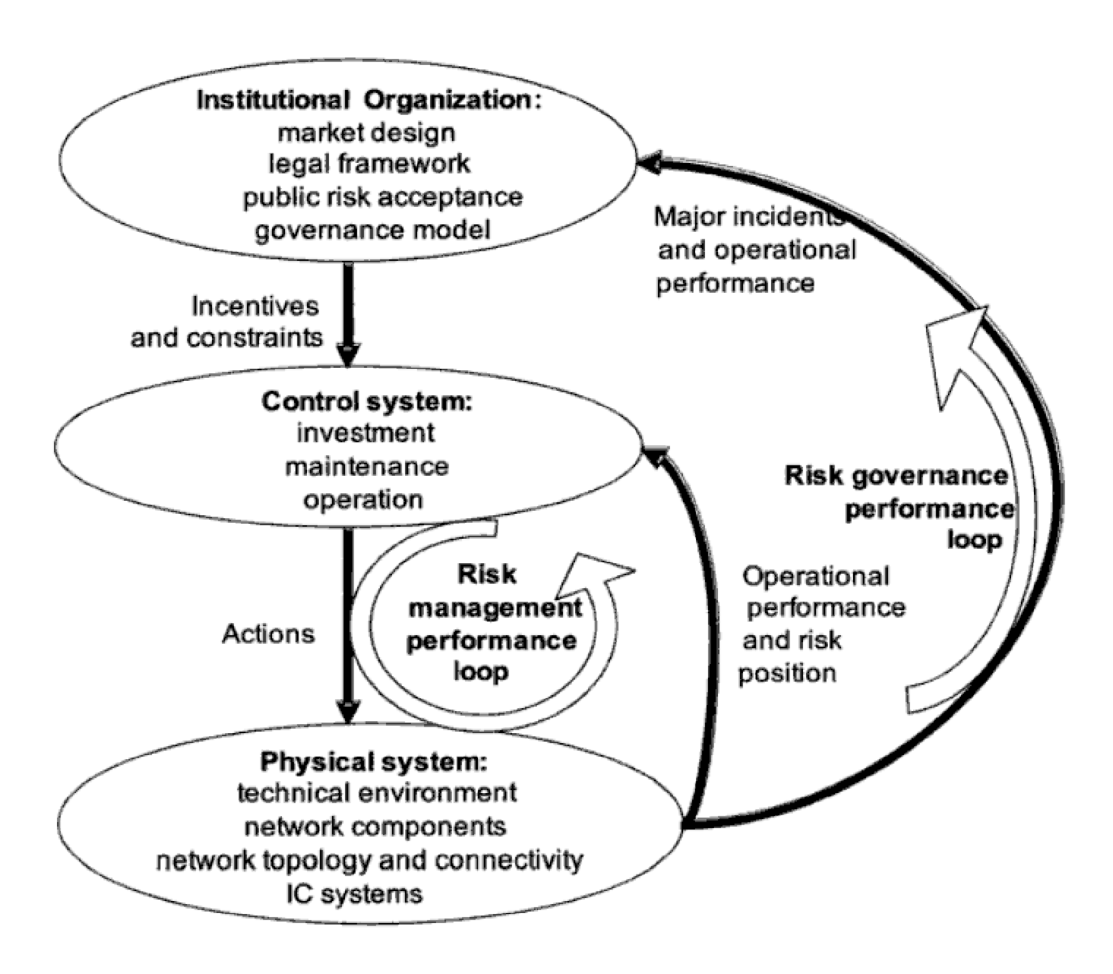



**Abbildung 36: Risk Management und Risikosteuerung**

Quelle: (Gheorge et al., 2006, S. XX)

Dabei handelt es sich bei der untersten Ebene um das physische System aus Komponenten zur Stromversorgung. Die zweite Ebene bildet das Kontrollsystem. Hier sind die Betreiber der Infrastruktur in den verschiedenen Bereichen von der Erzeugung bis zum Verbrauch vereint. In der obersten Ebene letztendlich handelt es sich um den institutionellen Rahmen, der auch im Rahmen der Anfälligkeit (siehe Kapitel 4.2 und 6.2) behandelt wurde. Insgesamt werden dabei durch *Risk Governance* alle Ebenen erfasst, während die oben genannten *Risk Management* Ansätze als Teil des Risk Governance auf den beiden unteren Ebenen angewendet werden können. Hier wird auch deutlich, dass Regierungen das System nur bedingt durch Anreize und Einschränkungen beeinflussen können, was insbesondere durch die Privatisierung weiter Teile des Systems bedingt ist. (Masera et al., 2006b, S. 136 ff)





# 7 Fazit

Der State of the Art der Forschung zur Verwundbarkeit Kritischer Infrastrukturen am Beispiel Stromausfall wurde im Rahmen dieser Studie anhand der Komponenten *Exposition*, *Anfälligkeit* und *Bewältigungskapazität* analysiert und im jeweiligen Bereich wurden Handlungsoptionen aufgezeigt.

Im Rahmen der Exposition von KRITIS wurde dabei zwischen Naturgefahren, Terroranschlägen und Cyberattacken als mögliche Ursache für einen Stromausfall unterschieden. Während unter den Naturgefahren Sturmfluten und Hochwasser die beiden einzigen sind, die gut räumlich eingrenzbar sind, können sich beispielsweise Hitzewellen oder Stürme über weite Bereiche erstrecken. Auch der Ort ihres Auftretens ist kaum im Vorhinein abzusehen. Handlungsoptionen im Rahmen der Exposition gegenüber Naturgefahren sind daher in zweierlei Hinsicht möglich: Gegenüber Hochwasser und Sturmfluten, in denen mögliche Expositionsgebiete gut definiert werden können, können Komponenten aus dem Gebiet hinaus verlegt oder bei Bedarf entsprechen geschützt werden. Gegenüber Naturgefahren, die schwer räumlich abgrenzbar sind, ist insbesondere die Verlegung von Erdkabeln eine Möglichkeit für den Schutz der Netze.

Terroranschläge auf die Stromversorgung werden hauptsächlich im Zusammenhang mit Atomkraftwerken thematisiert, da ein erfolgreicher Anschlag hier eine besonders starke Betroffenheit der Bevölkerung zur Folge hätte. Für die Auswirkung auf die Stromversorgung wird der Ausfall eines Kraftwerkes jedoch vermutlich keine starke Relevanz haben. Jedoch ergeben sich durch die immer stärkere Vernetzung der KRITIS mit dem Internet auch neue Möglichkeiten für Terroristen und Hacker, die in SCADA-Systeme eindringen und so möglicherweise die Steuerung der Elektrizitätsversorgung beeinflussen könnten. Hier müssen Angriffmöglichkeiten durch neue Technologien wie die Smart Grids berücksichtigt werden. Die Beurteilung der Gefährdungslage ist jedoch in der wissenschaftlichen Literatur umstritten. Allerdings bestehen auch hier Schutzmöglichkeiten, um die Exposition der Versorgung gegenüber solchen Angriffen zu reduzieren, wozu insbesondere die Verwendung sicherer Softwareprodukte und SCADA-Systeme gehören, die möglichst keine Angriffsflächen für Hacker bieten und die Verbesserung der Sicherheit von Schnittstellen mit dem Internet.

Die Analyse der Einflussfaktoren auf die Anfälligkeit der Elektrizitätsversorgung lässt sich in verschiedene Hauptbereiche unterscheiden. Als Herausforderungen sind hier der schwindende Einfluss des Staates, bedingt durch die zunehmende Privatisierung der Versorger, und die durch die Liberalisierung entstandene, starke Zersplitterung der Akteure zu nennen. Auch wirken sich gesellschaftliche Faktoren wie die Verschiebungen in der Nachfrage und der demographische Wandel auf die Versorgung aus. Die Komplexität des Systems selber und die Abhängigkeit von IT-Infrastrukturdienstleitungen haben zudem ebenso Einfluss auf die Verwundbarkeit des Systems, wie mangelnde Speichermöglichkeiten für Strom, sodass die



Produktion *just in time* in weiten Teilen notwendig ist und nicht auf Vorräte zurückgegriffen werden kann. In diesem Zusammenhang sollte die Verwendung neuer Technologien zu Speicherkapazitäten und zur Reduktion der Komplexität geprüft werden. Dies gilt auch im Hinblick auf Alternativen zu häufig verwendeten Sicherheitsstandards, wie beispielsweise Redundanzen, die in der Vergangenheit Stromausfälle wie im Emsland nicht verhindern konnten. Als Erweiterung des (n-1)-Standards wird in der Literatur insbesondere auf den besseren Austausch von Echtzeit-Daten hingewiesen, der es zudem dem Personal in Kontrollstellen leichter macht in Notfallsituationen alternative Entscheidungen zu treffen. Die Schulung von Mitarbeitern durch szenarien-basierte Übungen kann diese Entscheidungsfindung optimieren.

Grundsätzlich sollte ferner geprüft werden, ob durch neue Organisationsstrukturen der innereuropäische Stromhandel besser koordiniert werden kann und im Rahmen welcher Institution diese engere Kooperation möglich wäre. Auch die Möglichkeiten der Entwicklung neuer Normen und damit der Verpflichtung der Betreiber sollten überdacht werden. Hier stellen die unterschiedlichen Interessen zwischen Betreibern mit Tendenz zur Einsparung der Kosten, den Verbrauchern, die niedrige Strompreise erwarten und der Netzsicherheit eine Hauptherausforderung dar.

Die Bewältigungskapazität der Stromversorgung kann grob in zwei Kategorien unterteilt werden. Zum einen in technische, präventive Maßnahmen, und zum anderen in reaktive Maßnahmen, die den Umgang mit Notfallsituationen betreffen. Dabei können verschiedene Indikatoren herangezogen werden, wobei das *Umfeld*, also die stabilen politischen Verhältnisse und die *Dezentralisierung* des Systems Faktoren sind, die sich präventiv positiv auf die Bewältigungskapazität des Systems auswirken können. *Redundanzen*, die *Reduktion des Wiederherstellungsaufwandes* von Komponenten und Prozessen und die *Bereitschaft*, also der Grad der Vorbereitung auf Notfallsituationen, beispielsweise durch Übungen, sind Indikatoren für die reaktive Bewältigungskapazität. Ein sinnvoller Ansatz besteht hierbei in den regelmäßig durchgeführten LÜKEX-Übungen.

Da die Sicherung einer stabilen Elektrizitätsversorgung viele verschiedene Akteure aus Wirtschaft, Politik und Gesellschaft mit einschließen muss, ist die Betrachtung von Risk Governance Ansätzen zur Reduktion der Verwundbarkeit der Stromversorgung sinnvoll. Das gilt auch deswegen, weil die Konzeptualisierung des Risikos die Verwundbarkeit um die Komponente der Wahrscheinlichkeit des Eintretens einer Gefahr erweitert (Risiko = f (Gefahr, Verwundbarkeit)). Nach einem Abschätzungsprozess muss das akzeptierbare Restrisiko festgelegt werden und anschließend Management-Maßnahmen auf verschiedenen Ebenen (technische Ebene, Kontroll-Ebene und institutionelle Ebene) ergriffen werden, für die Handlungsmöglichkeiten im Rahmen dieser Studie vorgestellt worden sind.

Insgesamt lässt sich jedoch festhalten, dass die Forschung im Bereich Kritische Elektrizitätsinfrastruktur, einschließlich der Problembereiche Komplexität und Abhängigkeiten anderer



KRITIS von der Stromversorgung in Deutschland bisher wenig behandelt wurde. Zwar existieren erste Ansätze, wie beispielsweise der von Rinaldi et al. (2001), die sich dem Thema Komplexität und der Klassifizierung von Abhängigkeiten widmet, jedoch bleiben diese vage und bieten keine Lösungsansätze an. Ganzheitliche wissenschaftliche Ansätze, die die Verwundbarkeit der Elektrizitätsversorgung in ihrem Gesamtrahmen betrachten gibt es hingegen nur einige wenige (beispielsweise Kröger, 2008; Hellström, 2007 oder Gheorghe, 2006).

Zwar wurden die größeren Stromausfälle der Vergangenheit von den Betreiber untersucht; Berichte sind beispielsweise über die Bundesnetzagentur (Emsland im November 2006) oder die UCTE (2007) erhältlich. Jedoch fehlt es an einer systematischen und vergleichenden Auswertung aller Ereignisse. Entsprechend bleibt unklar, ob bestimmte Komponenten oder Prozesse besonders anfällig sind, sodass sich auch die Priorisierung von Handlungsmaßnahmen schwierig gestaltet. Ein erster Überblick über die Ereignisse der Vergangenheit zeigt zudem, dass Stromausfälle häufig nicht auf eine einzelne Ursache zurückzuführen sind.

Der geringe Umfang der wissenschaftlichen Grundlagen zum Thema Kritische Elektrizitätsversorgung und Stromausfall lässt sich dabei damit erklären, dass es sich um ein relativ junges Thema handelt, dass zunächst in den USA durch die Anschläge auf das World Trade Center 1993 und weiterer Terroranschläge zur Veröffentlichung des ersten Berichtes der *President's Commission on Critical Infrastructure Protection* führte. Mit der Gründung der interministeriellen Arbeitsgruppe Kritische Infrastrukturen AG KRITIS 1997, den Publikationen des BMI (2005, 2009) und dem Grünbuch der Arbeitsgemeinschaft „Öffentliche Sicherheit“ rückt das Thema auch in Deutschland immer mehr ins Zentrum der Aufmerksamkeit von Politik und Wissenschaft. Dies ist dabei auch deshalb von Vorteil, da sich im Zuge der Umstrukturierung der Elektrizitätsversorgung im Rahmen des Klimaschutzes und der Ressourcenknappheit, die zwangsläufig auch mit neuen Investitionen verbunden ist, zwar die Verwundbarkeit verändert, sich jedoch auch neue Möglichkeiten zur Reduktion der Verwundbarkeit ergeben. So beispielsweise durch die Dezentralisierung der Versorgung, insbesondere durch erneuerbare Energien, die durch die Inkonsistenz in der Erzeugung neue Speichertechnologien und Ansätze zur Nachfragesteuerung mit sich bringen. Neben den oben genannten Handlungsoptionen sollte daher ein Schwerpunkt der Forschung auf die Möglichkeiten der Verwundbarkeitsreduktion im Rahmen der erneuerbaren Energien und des damit einhergehenden Umbaus der Netze gelegt werden, um nachhaltige Investitionen zu sichern.





# Anhang 1: Dimensionen der Wirkzusammenhänge nach Rinaldi et al. (2001)

| **Dimension der Wirkungszusammenhänge** | **Erläuterung** |
|---|---|
| **Gegenseitige Abhängigkeit** | |
| Physisch | zwei Komponenten sind gegenseitig auf den materiellen Output der jeweils anderen angewiesen (z.B. Bahn und Kohlekraftwerk) |
| Cyber | eine Komponente ist abhängig von den Informationen einer anderen (Beispiel: Elektrizitätsversorgung und IT-Überwachung) |
| Geographisch | ein Umweltereignis hat Folgen in mehreren Infrastrukturen |
| Logisch | Abhängigkeit, die nicht auf physischer oder IT-Abhängigkeit beruht, in der auch menschliche Entscheidungen eine große Rolle spielen können (Beispiel: Urlauber verursachen Staus indem sie alle dann fahren, wenn das Benzin günstig ist) |
| **Umfeld der Infrastruktur** | |
| Ökonomische und betriebswirtschaftliche Möglichkeiten und Bedenken | z.B. Kosten für den Unterhalt der Systeme, technologische Verbesserungen oder sich verändernde Nachfrage |
| Politische Rahmenbedingungen | z.B.Energie-, Sicherheits- und Wirtschaftspolitik eines Landes |
| Entscheidungen der Regierung bezüglich Infrastruktur-Investitionen | z.B. Investitionen in Telekommunikationsinfrastruktur |
| Rechtliche Belange | z.B. Vorschriften zu Standards der Infrastruktur |
| Öffentliche Sicherheit | z. B. Umweltstandards zur Reduzierung der Luftverschmutzung oder Verbesserung der Notfallhilfe |



| | |
|---|---|
| Technik- und Sicherheitsbelange | Computerisierung und Automatisierung der Infrastrukturen benötigen neue Sicherheitskonzepte |
| Soziale und politische Angelegenheiten | Infrastrukturen sind heutzutage international verflochten und benötigen daher soziales wie politisches Feingefühl |
| **Verknüpfung und Reaktion** | |
| Verknüpfungsart (lose oder eng) | Ob lose oder enge Verknüpfungen vorherrschen legt fest, ob Infrastrukturen im Stressfall unflexibel oder anpassungsfähig sind. Enge Verknüpfung zwischen Infrastrukturen bedeutet hohe Abhängigkeit voneinander, während lose Verknüpfungen eher Unabhängigkeit versteht. |
| Verknüpfungsgrad (komplex oder linear) | Unter linearer Verknüpfung versteht man das Zusammenwirken vergleichbar mit einer Fließbandfertigung. Während komplexe Verknüpfungen ein Interagieren mit anderen Elementen außerhalb der normalen Kette verstehen. Z.B. Rückkopplungen und Verzweigungen zwischen zwei linearen Komponenten |
| Anpassungsfähigkeit vs. Inflexibilität | Faktoren, die die Anpassungsfähigkeit erhöhen, sind z.B. Trainings- und Bildungsprogramme, Datensicherungssysteme oder Notfallpläne. Demgegenüber stehen Faktoren, die Infrastrukturen unflexibel werden lassen. (restriktives System, Gesundheits- und Sicherheitsstandards oder feste Netzwerkstrukturen) |
| **Charakteristika der Infrastruktur** | |
| Räumliche Ebene | Innerhalb eines Infrastruktursystems gibt es eine räumliche Hierarchie, die je nach Betrachtungseben von der kleinsten Komponente des Systems (Einzelteil) bis hin zur Metastruktur (Verflechtung von Infrastrukturen) reicht. |
| Zeitliche Ebene | Zeigt eine große Spannweite auf. Besonders für Modelle und Simulationen sind die Zeitdimensionen wie beispielsweise Millisekunden |



| | |
|---|---|
| | (Energieversorgung) und Jahre (Infrastrukturverbesserungen) von besonderer Bedeutung. |
| Betriebsspezifischer Faktor | Beeinflusst, wie Infrastrukturen auf Ereignisse reagieren. Beinhaltet Arbeitsabläufe, Mitarbeitertraining oder Notfallpläne. |
| Organisationsstruktur | Beispielsweise internationaler Besitz, privater vs. staatlicher Besitz oder die Auswirkungen der Globalisierung haben wiederum starken Einfluss auf die betriebsspezifischen Charakteristika |
| **Art des Ausfalls** | |
| Kaskadenartiger Ausfall | Ein Zwischenfall in einer Infrastruktur führt zum Ausfall einer Komponente einer zweiten Infrastruktur (z.B. Stromausfall in Westeuropa 2006) |
| Ausfall mit sich verstärkenden Folgen | Der Ausfall einer Infrastruktur hat verstärkende Wirkung auf einen unabhängigen Ausfall einer zweiten Infrastruktur (z.B. Ausfall des Telekommunikationssystems und Ausfall in einem Büro => Ausfall im Transportsystem und somit verspätete Ankunft des Reparaturservices) |
| Ausfall aufgrund einer gemeinsamen Ursache | Zwei oder mehr Infrastrukturnetzwerke fallen zur selben Zeit aufgrund eines Einzelereignisses aus. (Beispiel: Telefon- und Energieleitungen verlaufen oftmals parallel zu Bahngleisen. Bei einer Zugentgleisung kann es zu Schäden in beiden Infrastrukturen kommen) |
| **Art des Betriebes** | |
| normal, während eines Ausfalls (*disruption*) oder zur Zeit der Instandsetzung (*repair*) | Je nachdem in welchem Zustand sich der Betrieb einer Infrastruktur befindet (normal, während eines Ausfalls oder zur Zeit der Instandsetzung) unterscheiden sich die Auswirkungen eintretender Ereignisse. |





# 8 Literaturverzeichnis

Adger, W. N. (2006). Vulnerability. *Global Environmental Change, 16*, 268–281.

Ajodhia, V. (2006). Costs of Power Infrastructure Malfunctioning. In A. Gheorghe, M. Masera, M. Weijnen & L. De Vries (Hrsg.). *Critical Infrastructures at Risk. Securing the European Electric Power System* (331-342). Dordrecht: Springer.

Alkassar, A., Garschhammer, M., Gehring, F., Keil, P., Kelter, H., Löwer, U., Pankow, M., Sadeghi, A.-R., Schiffers, M., Ullmann, M. & Vogel, S. (2003). *Kommunikations- und Informationstechnik 2010+3: Neue Trends und Entwicklungen in Technologien, Anwendungen und Sicherheit.* Bundesamt für Sicherheit in der Informationstechnik (BSI). Verfügbar unter https://www.bsi-fuer-buerger.de/ContentBSI/Publikationen/Studien/trend2010/index_htm.html [29. August 2010].

Alvaro, A. (2009). Sicherheit in der Informationsgesellschaft. In P. Rösler & C. Lindner (Hrsg.). *Freiheit: gefühlt - gedacht - gelebt. Liberale Beiträge zu einer Wertediskussion* (S. 214 - 227). Wiesbaden: VS Verlag.

Amin, M. (2000). National Infrastructures as Complex Interactive Systems. In T. S. Weyrauch (Hrsg). *Automation, Control, and Complexity* (S. 263-286). Chichester: John Wiley and Sons.

Antrag der Fraktion GRÜNE und Stellungnahme des Wirtschaftsministeriums (2005). *Sicherheitsmängel bei Strommasten des baden-württembergischen Freilandleitungsnetze*. Landtag von Baden-Württemberg, 13. Wahlperiode.

Anwar, H. Z., Post, J., Strunz, G., Birkmann, J. & Gebert, N. (2008). Role of Community's Vulnerability at Local Level and its Contribution to Tsunami Risk in Indonesia: Study Case at Padang Municipality. *International Conference on Tsunami Warning (ICTW)* (S. 8). Bali.

Ashmore, W. C. (2009). Impact of Alleged Russian Cyber Attacks. *Baltic Security & Defence Review, 11*. 5-40.

Bacher, R. & Näf, U. (2003). *Bericht über den Stromausfall in Italien am 28. September 2003.* Bern: Bundesamt für Energie BFE.

Baker, G. H. (2005). A Vulnerability Assessment Methodology for Critical Infrastructure Facilities. *DHS Symposium: R&D Partnerships in Homeland Security*. Boston.

Bender, P. (2010). *Die Gas-Pipeline von Russland nach Deutschland.* Verfügbar unter http://politik.germanblogs.de/archive/2010/01/17/die-gas-pipeline-von-russland-nach-deutschland.htm [14. September 2010].



Benzin, A. (2005). *Versicherungstechnische Bewertung unterschiedlicher Deckungskonzepte für Terrorismusrisiken.* Karlsruhe: Verlag Versicherungswirtschaft.

Birkmann, J. (2006). Measuring vulnerability to promote disaster-resilient societies: Conceptual frameworks and definitions . In J. Birkmann (Hrsg). *Measuring Vulnerability to Natural Hazards: Towards Disaster Resilient Societies* (9-54). New York: United Nations University Press.

Birkmann, J. & Krings, S. (2008). Die Vulnerabilität kritischer Infrastrukturen gegenüber (möglichen) Auswirkungen des Klimawandels. *Zeitschrift Notfallvorsorge , 4*, 25-30.

Birkmann, J., Tetzlaff, G. & Zentel, K.-O. (2009). *Addressing the Challenge: Recommendations and Quality Criteria for Linking Disaster Risk Reduction and Adaptation to Climate Change.* Bonn: Deutsches Komitee Katastrophenvorsorge.

Birkmann, J., Dech, S., Gähler, M., Krings, S., Kühling, W., Meisel, K., et al. (in Druck). *Abschätzung der Verwundbarkeit gegenüber Hochwasserereignissen auf kommunaler Ebene* (Bde. Praxis im Bevölkerungsschutz, Band 4). (B. f. (BBK), Hrsg.) Bonn.

Bitsch, R. (2006). Integration von erneurbaren Energiequellen und dezentralen Erzeugungen in bestehende Elektro-Energiesysteme. *Internet-Zeitschrift des Leibniz-Instituts für interdisziplinäre Studien e.V. (LIFIS)*, 1-15.

Blaikie, P. T., Cannon, I., Davis, B. & Wisner, B. (1994). *At Risk: Natural Hazards, People's Vulnerability and Disasters.* (1 Ausg.). London: Ruthledge.

Bohle, H.-G., & Glade, T. (2008). Vulnerabilitätskonzepte in Sozial- und Naturwissenschaften. In C. Felgentreff & T. Glade (Hrsg.). *Naturrisiken und Sozialkatastrophen* (99-119). Heidelberg: Spriger-Verlag.

Borst, D., Jung, D., Murshed, M. & Werner, U. (2006). Development of a methodology to assess man-made risks in Germany. *Natural Hazards and Earth System Sciences*, *6*, 779-802.

Bouffard, F. & Kirschen, D. S. (2008). Centralised and distributed electricity systems. *Energy Policy*, *36 (12)*, 4504-4508.

Bouwmans, I., Weijnen, M. P. & Gheorghe, A. (2006). Infrastructure ar Risk. In A. V. Gheorghe, M. Masera, M. Weijnen & L. De Vries (Hrsg.). *Critical Infrastructure at Risk. Securing the Eruopean Electric Power System* (19-36). Dordrecht: Springer.

Brakelmann, H. (2006). *Stellungnahme zum Antrag der Fraktion BÜNDNIS 90/DIE GRÜNEN. Drucksache 60/710: Priorität für Erdkabel beim Ausbau der Stromnetze in Schleswig-Holstein.* Duisburg: Schleswig-Holsteinischer Landtag Umdruck 16/972.



Bräuninger, M., Schröer, S. & Schulze, S. (2010). *Power für Deutschland - Energieversorgung im 21. Jahrhundert.* (3. Auflage). Hamburg: UniCredit Bank AG.

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) (2005). *Problemstudie: Risiken für Deutschland. (Teil 2).* Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, Akademie für Krisenmanagement, Notfallplanung und Zivilschutz (AKNZ). Bad Neuenahr-Ahrweiler: WissenschaftsForum.

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) (2010a). *Der Stromausfall und seine Auswirkungen*. Verfügbar unter http://www.bbk.bund.de/nn_402322/DE/00__Home/TopThema/TT__2010/Stromausfall-und-Auswirkungen.html [18. August 2010].

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) (2010b). *Übungsserie LÜKEX*. Verfügbar unter http://www.denis.bund.de/luekex/ [26. August 2010].

Bundesamt für Sicherheit in der Informationstechnik (BSI) (2009). *Die Lage der IT-Sicherheit in Deutschland 2009.* Bonn: Bundesamt für Sicherheit in der Informationstechnik.

Bundesamt für Sicherheit in der Informationstechnik (BSI) (o.J.). *IT-Grundschutz-Kataloge*. Verfügbar unter https://www.bsi.bund.de/cln_183/ContentBSI/grundschutz/kataloge/kataloge.html [14. August 2010].

Bundesamt für Strahlensicherheit (BfS) (2010). *Kerntechnik: Meldepflichtige Ereignisse: Internationale Bewertungsskala (INES)*. Verfügbar unter http://www.bfs.de/de/kerntechnik/ereignisse/ines.html [15. September 2010].

Bundesamt für Strahlensicherheit (BfS) (o.J.). *Kernkraftwerke in Deutschland - Meldepflichtige Ereignisse seit Inbetriebnahme.* Verfügbar unter http://www.bfs.de/de/kerntechnik/ereignisse/standorte/karte_kw.html [10. September 2010].

Bundeskriminalamt (BKA) (2010). *IuK-Kriminalität - Bundeslagebericht 2009.* Wiesbaden: Bundeskriminalamt.

Bundesministerium des Inneren (BMI) (2003). Schutz kritscher Infrastrukturen. Unterrichtung des BMI zu Einzelaspekten. In BMI (Hrsg.). *Nach dem 11. September 2001. Maßnahmen gegen den Terror* (245-247). Berlin: Bundesministerium des Inneren.

Bundesministerium des Inneren (BMI) (2005). *Schutz Kritischer Infrastrukturen – Basisschutzkonzept: Empfehlungen für Unternehmen.* Berlin: Bundesministerium des Inneren.



Bundesministerium des Inneren (BMI) (2009). *Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie).* Berlin: Bundesministerium des Innern.

Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit (BMU) (2006). *Energieversorgung für Deutschland.* Berlin: Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit.

Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit (BMU) (2009). *Roadmap Energiepolitik 2020: Zehn Leitsätze.* Verfügbar unter http://www.bmu.de/files/bilder/allgemein/image/jpeg/roadmap_energie_netzbetr.jpg [19.September 2010].

Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit (BMU) (2010). *Erneuerbare Energien in Zahlen. Nationale und internationale Entwicklung.* Berlin: Bundeministerium für Umwelt, Naturschutz und Reaktorsicherheit.

Bundesministerium für Wirtschaft und Technologie (BMWi) (2010). *E-Energy. Auf dem Weg zum Internet der Energie.* Berlin: Bundesministerium für Wirtschaft und Technologie.

Bundesministerium für Wirtschaft und Technologie (BMWi) & Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit (BMU) (2006). *Energieversorgung für Deutschland. Statusbericht für den Energiegipfel am 3. April 2006.* Berlin.

Bundesnetzagentur. (2006a). *Untersuchungsbericht über die Versorgungsstörungen im Netzgebiet des RWE im Münsterland vom 25.11.2005.* Bonn: Bundesnetzagentur.

Bundesnetzagentur (2006b) *Monitoringbericht 2006 der Bundesagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahn.* Verfügbar unter http://www.bundesnetzagentur.de/cae/servlet/contentblob/31292/publicationFile/1122/Monitoringbericht2006Id7263pdf.pdf [02. September 2010].

Bundesnetzagentur. (2007). *Bericht der Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahhn über die Systemstörung im deutschen und europäischen Verbundsystem am 4. November 2006.* Bonn: Bundesnetzagentur.

Bundesnetzagentur (2008) *Monitoringbericht 2008.* Verfügbar unter http://www.bundesnetzagentur.de/cae/servlet/contentblob/97436/publicationFile/1106/Monitoringbericht08EnergieId14513pdf.pdf [06. September 2010].

Bundesnetzagentur. (2009). *Monitoringbericht 2009.* Bonn: Bundesnetzagentur.

Bundesnetzagentur (2010). *Versorgungsqualität – SAIDI-Wert 2008.* Verfügbar unter http://www.bundesnetzagentur.de/DE/Sachgebiete/ElektrizitaetGas/Sonderthemen/SAIDIWertStrom2008/SAIDIWertStrom2008_node.html [13. September 2010].



Bundesverband der Energie- und Wasserwirtschaft (BDEW) (2009). *Abschlussbericht Projektgruppe Intelligente Netz / Smart Grids, Arbeitsergebnisse von 10/08-3/09.* Berlin: Bundesverband der Energie- und Wasserwirtschaft.

Bundesverband der Energie- und Wasserwirtschaft (BDEW) (2010a). *Brutto-Stromerzeugung nach Energieträgern.* Verfügbar unter http://www.bdew.de/bdew.nsf/id/DE_Bruttostromerzeugung_in_Deutschland/$file/Bruttostromerzeugung%20in%20Deutschland%202009.pdf [16. September 2010].

Bundesverband der Energie- und Wasserwirtschaft (BDEW) (2010b). *BDEW-Fakten*. Verfügbar unter http://bdew.de/bdew.nsf/id/DE_20100322_PM_Deutsches_Stromnetz_ist_178_Millionen_Kilometer_lang/$file/Fakten_BDEW_Stromnetze.pdf [16. September 2010].

Cardona, O. (2006). A system of indicators for disaster risk management in the Americas. In J. Birkmann (Hrsg.). *Measuring Vulnerability to Natural Hazards. Towards Disaster Resilient Societies* (S. 189-209). New York: United Nations University Press.

CONSENTEC, EWI, IAEW (2008). *Analyse und Bewertung der Versorgungssicherheit in der Elektrizitätsversorgung. Untersuchung im Auftrag des Bundesministerium für Wirtschaft und Technologie (BMWi).* Bonn.

Dederichs, S. (2010). *Wo Server sicher sind-Besuch im 1&1 Rechenzentrum*. Verfügbar unter http://blog.1und1.de/2010/04/15/wo-server-sicher-sind-besuch-im-karlsruher-11-rechenzentrum/ [02. September 2010].

Deutscher Bundestag (2010). Gesetz zur Neuregelung des Rechts der Erneuerbaren Energien im Strombereich und zur Änderung damit zusammenhängender Vorschriften (Erneuerbare-Energien-Gesetz, EEG 2009), amtliche Fassung vom 25. Oktober 2008. *Bundesgesetzblatt (41)*, 2074-2100.

Energie Baden-Württemberg (EnBW) (2008). *Stromausfall in Karlsruhe nach technischem Defekt.* Stuttgart: EnBW.

Denning, D. E. (2001). Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. In J. Arquilla & D. Ronfeldt (Hrsg.). *Networks and Netwars* (S. 239-288). Santa Monica: RAND.

Deutsche Energie-Agentur (dena) (2005). *Energiewirtschaftliche Planung für die Netzintegration von Windenergie in Deutschland an Land und Offshore bis zum Jahr 2020 (dena-Netzstudie).* Berlin: Deutsche Energie-Agentur.



Deutsches Komitee Katastrophenvorsorge (DKKV) (2003). *Hochwasservorsorge in Deutschland. Lernen aus der Katastrophe 2002 im Elbeeinzugsgebiet.* Bonn: Deutsches Komitee Katastrophenvorsorge.

De Vries, L., De Jong, M., De Bruijne, G. H., & Knops, H. (2006). Liberalisation and Internationalisation of the European Electricity Supply System. In A. Gheorghe, M. Masera, M. Weijnen & L. De Vries (Hrsg.). *Critical Infrastructures at Risk* (37-83). Dordrecht, Netherlands: Springer.

Die Bundesregierung. (2008). *Deutsche Anpassungsstrategie an den Klimawandel vom Bundeskabinett am 17. Dezember 2008 beschlossen.* Berlin: Die Bundesregierung.

Dunham, K. & Melnick, J. (2009). *Malicious Bots - An Inside Look into the Cyber-Criminal Underground of the Internet.* Boca Raton: Auerbach Publications.

Einarsson, S. & Rausand, M. (1998). An Approach to Vulnerability Analysis of Complex Industrial Systems. *Risk Analysis, 18* (5), 535-546.

Europäische Kommission (2004). *Mitteilung der Kommission an den Rat und das europäische Parlament. Abwehrbereitschaft und Folgenbewältigung bei der Terrorismusbekämpfung.* Brüssel: EU-Kommission.

Europäische Kommission (2005). *Parlamentsmaterialien*. Verfügbar unter http://www.bundesrat.de/cln_179/SharedDocs/Drucksachen/2005/0501-600/575-05,templateId=raw,property=publicationFile.pdf/575-05.pdf [25. August 2010].

Europäische Kommission (2005). Grünbuch über ein europäisches Programm für den Schutz Kritischer Infrastrukturen. *KOM(2005) 576 endgültig* . Brüssel.

Europäische Kommission (2006). Mitteilung der Kommission über ein Europäisches Programm für den Schutz kritischer infrastrukturen. *KOM(2006) 786 endgültig* . Brüssel.

Europäische Kommission (2008). *Vorschlag für eine Entscheidung des Rates über ein Warn- und Informationsnetz für kritische Infrastrukturen (CIWIN), KOM(2008) 676 endgültig.* Brüssel.

Europäischer Rat (2008). RL 2008/114/EG über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern. Brüssel.

European Commission. (2006). *European Technology Plattform Smart Grids. Vision and Stategy for Europe´s Electricity Networks of the Future.* Brüssel: European Commission.

European Network of Transmission System Operators for Electricity (ENTSO-E) (o. J.). *Statistical Yearbook 2008.* Brüssel.



Fischedick, M., Supersberger, N. & Zeiss, C. (2009). *Hindernis Atomkraft. Die Auswirkungen einer Laufzeitverlängerung der Atomkraftwerke auf erneuerbare Energien.* Berlin: Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit.

Fischer, W. (2007). *www.InfrastrukturInternet-Cyberterror.Netzwerk. Analyse und Simulation strategischer Angriffe auf die kritische Infrastruktur Internet.* Jülich: Forswchungszentrum Jülich.

focus-online (2006). *Schnee-Chaos. Umgeknickte Strommasten im Münsterland.* Verfügbar unter http://www.focus.de/panorama/welt/schnee-chaos_did_11852.html [28. September 2010].

focus-online (2010). *Atomkraftwerke. Union und FDP beschließen Laufzeitverlängerung für Atommeiler*. Verfügbar unter http://www.focus.de/politik/weitere-meldungen/atomkraftwerke-union-und-fdp-beschliessen-laufzeitverlaengerung-fuer-atommeiler_aid_549016.html [17. Seotember 2010].

Fritzon, A., Ljungkvist, K., Boin, A. & Rhinard, M. (2007). Protecting Europe's Critical Infrastructures: Problems and Prospects. *Journal of Contingencies and Crisis Management, 15*, 30-41.

Geier, W., Hentschel, T. & Hidajat, R. (2005). *Problemstudie: Risiken für Deutschland, Teil 1*. Bonn: Bundesamt für Bevölkerungsschutz und Katastrophenhilfe.

Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) (o.J.). *INES – International Nuclear Event Scale*. Verfügbar unter http://www.grs.de/content/ines-information-auf-einen-blick [25.August 2010].

Gheroghe, A. V., Masera, M., Weijnen, M. & De Vries, L. (2006). *Critical Infrastructure at Risk. Securing the European Electric Power System.* Dordrecht: Springer.

Gorelova, A. (2010). *Smart Grid - Das intelligente Stromnetz. Eine Einführung. Was es ist, wie es funktioniert und welche Folgen es für uns hat.* Frankfurt am Main: Steubing AG Research.

Gorman, S. (2009). *Electricity Grid in U.S. Penetrated By Spies.* The Wall Street Journal. Verfügbar unter http://online.wsj.com/article/SB123914805204099085.html [12.September 2010].

Greve, H. (2009). Kritische Infrastrukturen. *Datenschutz und Datensicherheit, 33 (12),* 756-758.

Haas, R. & Redl, C. (2009). *Langfristige Szenarien der gesellschaftlich optimalen Stromversorgung der Zukunft.* Wien: Bundesministerium für Verkehr, Innovation und Technologie.



Haber, A. & Bliem, M. G. (2010). Smart Grids - Auswirkungen auf die Netzentgelte. *Energiewirtschaftliche Tagesfragen, 1/2,* 2-5.

Hammons, T. J. (2008). Integrating renewable energy sources into European grids. *Electrical Power and Energy Systems, 30,* 462-475.

Hanning, A. (2008). Deutsche Innensicherheitspolitik. Strategische Bedrohungen und ihre Abwehr. *Zeitschrift für Außen- und Sicherheitspolitik, 1 (1),* 36-45.

Hellström, T. (2007). Critical infrastructure and systemic vulnerability: Towards a planning framework. *Safety Science, 45,* 415-430.

Hiete, M., Merz, M., Trinks, C., Grambs, W. & Thiede, T. (2010). *Krisenmanagement Stromausfall. Krisenmanagement bei einer großflächigen Unterbrechung der Stromversorgung am Beispiel Baden-Württemberg.* Bonn: Bundesamt für Bevölkerungsschutz und Katastrophenhilfe.

Hohenemser, C., Kates, R., & Slovic, P. (1983). The Nature of Technological Hazard. *Science*, *220*, 378-384.

Holenstein, M. (2007). *Risikowahrnehmung Versorgungsqualität. Analyse und Empfehlungen aufgrund von Fokusgruppen-Gesprächen und Einzelinterviews zum Thema Stromausfall.* Winterthur: Stiftung Risiko-Dialog St. Gallen.

Holmgren, A. J. & Molin, S. (2006). Using Disturbance Data to Assess Vulnerability of Electric Power Delivery Systems. *Journal of Infrastructure Systems, 12 (4),* 243-251.

Holmgren, A. J. (2007). A Framework for Vulnerability Assessment of Electric Power Systems. In A. Murray & T. Grubesic (Hrsg.). *Critical Infrastructure. Reliability and Vulnerability* (31-55). Berlin: Springer-Verlag.

Horbaty, R. & Rigassi, R. (2007). *Steckdosenhybride: Fahrzeuge erbringen Regelungsleistungen im Stromnetz. Zusammenfassung der Vorstudie.* Bern: Bundesamt für Energie.

Hufelschulte, J. (2006). *Anschlag. Knapp am Tod vorbei.* Verfügbar unter http://www.focus.de/politik/deutschland/anschlag-knapp-am-tod-vorbei_aid_214199.html [19. September 2010].

Hussels, D. & Kießling, F. (2005). MS-Freileitung nach neuer Norm DIN EN 50423 (VDE 0210-10 bis -12). *etz Elektrotechnik + Automation, 12,* 34-40.

Intergovernmental Panel on Climate Change (IPCC) (2007a). Global Climate Projections. In S. Solomon, D. Qin, M. Manning, Z. Chen, M. Marquis, K.B. Averyt, M. Tignor & H.L. Miller (Hrsg.). Climate Change 2007: The Physical Science Basis. Contribution of Working



Group I to the Fourth Assessment Report of the Intergovernmental Panel on Climate Change (747 – 845). Cambridge: Cambridge University Press.

Intergovernmental Panel on Climate Change (IPCC) (2007b). Zusammenfassung für politische Entscheidungsträger. In S. Solomon, D. Qin, M. Manning, Z. Chen, M. Marquis, K.B. Averyt, M. Tignor & H.L. Miller (Hrsg). *Klimaänderung 2007: Wissenschaftliche Grundlagen. Beitrag der Arbeitsgruppe I zum Vierten Sachstandsbericht des Zwischenstaatlichen Ausschusses für Klimaänderung (IPCC)* (1-18). Cambridge: Cambridge University Press.

International Atomic Energy Agency (IAEA) (2010). *Home: Our Work: Nuclear Safety & Security: Emergency Preparedness: INES*. Verfügbar unter http://www-ns.iaea.org/tech-areas/emergency/ines.htm [15. September 2010].

International Risk Governance Council (IRGC) (2005). *White Paper on Risk Governance: Towards an Integrative Approach.* Geneva.

International Risk Governance Council (IRGC) (2006). *White Paper on Managing and Reducing Social Vulnerabilities from Coupled Critical Infrastructures.* Châtelaine.

International Risk Governance Council (IRGC) (2010). *Emerging Risks - Sources, drivers and governance issues* . Genf.

Kloepfer, M. (2010). *Schutz kritischer Infrastrukturen.* Baden-Baden: Nomos.

Koehler, G., Schwab, M., Hauff, V., Kluth, K., Finke, W. & Belz, J. (2006) Niedrigwasserperiode 2003 in Deutschland. Ursachen - Wirkungen - Folgen. *Mitteilungen der Bundesanstalt für Gewässerkunde (BfG), 27,* Koblenz.

Koppe, C., Kovats, S., Jendritzky, G. & Menne, B. (2004). *Heat-waves: risk and responses.* Kopenhagen: World Health Organization.

Krings, S. (im Druck). Verwundbarkeitsassessment der Strom- und Trinkwasserversorgung gegenüber Hochwasserereignissen. In J. Birkmann, S. Dech, M. Gähler, S. Krings, W. Kühling, K. Meisel, A. Roth, A. Schieritz, H. Taubenböck, M. Vollmer, T. Welle, J. Wolfertz, M. Wurm & H. Zwenzer (Hrsg). *Abschätzung der Verwundbarkeit gegenüber Hochwasserereignissen auf kommunaler Ebene* (21-47). Bonn: Bundesamt für Bevölkerungsschutz und Katastrophenhilfe.

Kröger, W. (2008). Critical infrastructures at risk: A need for a new conceptual approach and extended analytical tools. *Reliability Engineering and System Safety, 93,* 1781-1787.

Kropp, J., Holsten, A., Lissner, T., Roithmeier, O., Hattermann, F., Huang, S., Rock, J., Wechsung, F., Lüttger, A., Pompe, S., Kühn, I., Costa, L., Steinhäuser, M., Walther, C., Klaus, M., Ritchie, S. & Metzger, M. (2009). *Klimawandel in Nordrhein-Westfalen.*



*Regionale Abschätzung der Anfälligkeit ausgewählter Sektoren. Abschlussbericht.* Potsdam: Potsdam-Instituts für Klimafolgenforschung.

Kuhn, J. (2005). *Der Schutz kritischer Infrastrukturen. Unter besonderer Berücksichtigung von kritischen Informationsinfrastrukturen.* Hamburg: Interdisziplinäre Forschungsgruppe Abrüstung und Rüstungskontrolle.

Kuhn, J. & Neuneck, G. (2005). *Terrorgefahr und die Verwundbarkeit modernener Industriestaaten: Wie gut ist Deutschland vorbereitet.* Hamburg: Institute for Peace Research and Security Policy at the University of Hamburg.

Kurth, M. (2006). Stromausfall. *Pressekonferenz 17. November 2006* . Bonn: Bundesnetzagentur.

Küchle, H. (2009). Bedrohung und Schutz Kritischer Infrastrukturen an Häfen, Flughäfen und Bahnhöfen. *Zeitschrift für Außen- und Sicherheitspolitik, 1*, 14-23.

Lange, J. (2009). *Wärmelast Rhein.* Mainz: Bund für Umwelt und Naturschutz Deutschland.

Lauwe, P. & Riegel, C. (2008). Schutz Kritischer Infrastrukturen - Konzepte zur Versorgungssicherheit. *Informationen zur Raumentwicklung*, *1/2*, 113-125.

Lenz, S. (2009). *Vulnerabilität kritischer Infrastrukturen.* Bonn: Bundesamt für Bevölkerungsschutz und Katastrophenhilfe.

Leuschner, U. (2010). *Energie-Chronik. 100301.* Verfügbar unter http://www.udo-leuschner.de/energie-chronik/100301g1.gif [22. September 2010].

Masera, M., Stefanini, A. & Dondossola, G. (2006a). The Security of the Information and Communcation Systems and the E+I Paradigm. In A. Gheorghe, M. Masera, M. Weijnen & L. De Vries (Hrsg.). *Critical Infrastructures at Risk* (85-116). Dordrecht: Springer.

Masera, M., Wijnia, Y., de Vries, L., Kuenzi, C., Sajeva, M. & Weijnen, M. (2006b). Governing Risk in the European Critical Elictricity Infrastructure. In A. V. Gheorghe, M. Masera, M. Weijnen & L. De Vries (Hrsg.). *Critical Infrastructure at Risk* (117-152). Dordrecht: Springer.

McDaniel, P. & McLaughlin, S. (2009). Security and Privacy Challenges in the Smart Grid. *IEEE Security & Privacy, 7 (3),* 75-77.

McDaniels, T., Chang, S., Cole, D., Mikawoz, J. & Longstaff, H. (2008). Fostering resilience to extreme events within infrastructure systems: Characterizing decision contexts for mitigation and adaption. *Global Environmental Change, 18,* 310-318.



Melde- und Analysestelle Informationssicherung (MELANI) (2007). *Informationssicherung. Lage in der Schweiz und international.* Bern: Schweizerische Eidgenossenschaft.

Menski, U. & Gardemann, J. (2008). *Auswirkungen des Ausfalls Kritischer Infrastrukturen auf den Ernährungssektoram Beispiel des Stromausfalls im Münsterland 2005.* FH Münster. Akademie für Krisenmanagement, Notfallplanung und Zivilschutz (AKNZ).

HYPERLINK "http://www.merkur-online.de/index.html" \o "merkur-online" merkur-online (2007). *Hintergrund: Die schwersten Terroranschläge in Europa.* Verfügbar unter http://www.merkur-online.de/nachrichten/welt/hintergrund-schwersten-terroranschlaege-europa-355939.html [24. September 2010].

Merz, B. & Emmermann, R. (2006). Zum Umgang mit Naturgefahren in Deutschland: Vom Reagieren zum Risikomanagement. *GAIA: Reihe Naturgefahren, 4*, 265-274.

Metzger, J. (2004). *Das Konzept "Schutz kritischer Infrastrukturen" hinterfragt.* Zürich: Forschungsstelle für Sicherheitspolitik.

Meyer, K. (o.J.). Katastrophenfolgen und Folgekatastrophen. In M. Kloepfer & K. Meßerschmidt (Hrsg.). *Anmerkungen zum Katastrophenrecht. Dokumentation der Arbeitsgruppe "Katastrophen und Recht". 2. Gesellschaftswissenschaftliches Kolleg der Studienstiftung des deutschen Volkes* (60-65).

Möckli, D. (2010). *Cyberwar: Konzept, Stand bund Grenzen.* Zürich: Center for Security Studies (CSS).

Münchener Rück (2009): *Naturkatastrophen 2008 – Analysen, Bewertungen, Positionen, TopicsGeo.* München.

Oberweis, M. (2006). Die Elektrizitätsversorgung im Wandel der Zeit. *Revue Technique Luxembourgeoise, 1*, 25-29.

Odenthal, H. W. (2003). Der Schutz kritischer Infrastrukturen. In K. Hirschmann & C. Leggemann (Hrsg.) *Der Kampf gegen den Terrorismus. Strategien und Handlungserfordernisse in Deutschland* (281-316). Berlin: Berliner Wissenschafts-Verlag.

Oswald, B. (o.J.). *Technische Fragen der Netzverstärkung.* Hannover: Institut für Energieversorgung und Hochspannungstechnik ForWind Zentrum Windenergieforschung.

Ottmüller, M. & Nieder, T. (2010). *Entwicklung der erneuerbaren Energien in Deutschland im Jahr 2009. Grafiken und Tabellen Stand: Juli 2010 unter Verwendung aktueller Daten der Arbeitsgruppe Erneuerbare Energien-Statistik (AGEE-Stat).* Berlin: Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit.



Pelling, M. (2005). Measuring Vulnerability to Urban Natural Disaster Risk. *Open House International, Special Issue on Managing Urban Disasters, 31(1),* 125-132.

Perrow, C. (1987). *Normale Katastrophen: Die unvermeidbaren Risiken der Großtechnik.* Frankfurt / New York: Reihe Campus.

President's Commission on Critical Infrastructure Protection (PCCIP) (1997). *Critical Foundations - Protecting America's Infrastructure*. Verfügbar unter http://www.fas.org/sgp/library/pccip.pdf [24. September 2010].

Reason, J. (1994). *Menschliches Versagen.* Heidelberg: Spektrum.

Reichenbach, G., Wolff, H., Göbel, R. & Stokar von Neuforn, S. (2008). *Risiken und Herausforderungen für die öffentliche Sicherheit in Deutschland.* Berlin: Grünbuch des Zukunftsforums Öffentliche Sicherheit.

Renn, O. (2008). *Risk Governance.* London: Earthscan.

Renn, O., Schweizer, P.-J., Dreyer, M., & Klinke, A. (2007). *Risiko. Über den gesellschaftlichen Umgang mit Unsicherheit.* München.

Rheinisch-Westphälisches Elektrizitätswerk (RWE) (2006). *Redundanz in den Stromnetzen*. Verfügbar unter http://www.rwe.com/web/cms/de/37110/rwe/presse-news/pressemitteilung/?id=4000965&pmid=4000965&SiteSlaId=30000003 [26. August 2010].

Rieger, F. (2010). Der digital Erstschlag ist erfolgt. *Frankfurter Allgemeine Zeitung*. Nr. 220, S. 33.

Riepl, S. (2010). *Stromnetz im 20. Jahrhundert. So funktioniert das Stromnetz.*Verfügbar unter http://www.forum-netzintegration.de/66/?L=0 [19. September 2010].

Rinaldi, S. M., Peerenboom, J. P. & Kelly, T. K. (2001). Identifying, Understanding and Analysing Critical Infrastructure Interdependencies. *IEEE Control Systems Magazine*, *21 (6)* S. 12-25.

Rinaldi, S. M. (2004). *Modeling and Simulating Critical Infrastructures and Their Interdependencies.* NewYork: System Sciences.

Robles et. al. (2008). Vulnerabilities in SCADA and Critical Infrastructure Systems. *International Journal of Future Communication and Networking, 1 (1),* 99-104.

Saafan, A. (2009). *Distributed Denial of Service Attacks: Explanation, classification and suggested Solutions.* Verfügbar unter http://packetstormsecurity.nl/papers/ [22.09.2010].



Sam, K. (2009) *Stromnetz wird durch Smart Grid für Hacker anfällig. Flächendeckender Stromausfall wäre denkbar*. Presstext Austria. Verfügbar unter http://pressetext.at/news/090323002/stromnetz-wird-durch-smart-grid-fuer-hacker-anfaellig/ [23.August 2010].

Schäuble, W. (2010). Schutz kritischer infrastrukturen als Aufgabe der Politk. In M. Kloepfer (Hrsg.). *Schutz kritischer Infrastrukturen* (21-25). Baden-Baden: Nomos.

Schily, O. (2003). Es gibt keine Sicherheit ohne IT-Sicherheit. *Rede von Bundesinnenministers Otto Schily anlässlich der Fachkonferenz des „Münchener Kreises“*. München.

Schmid, J., Strauss, P., Hatziargyriou, N., Akkermans, H., Buchholz, B., Van Oostvoorn, F., Reyero, R. & Chadjivassiliadis (2005). *Towards Smart Power Networks. Lessons learned from European research FP5 projects.* Brüssel: European Commission.

Schmidt, J. & Vohrer, P. (2010). *Erneuerbare Energien und Grundlastkraftwerke - ein Systemkonflikt?* Berlin: Agentur für Erneuerbare Energien.

Schmidt-Preuß, M. (2010). Europäische und internationale Ansätze zum Schutz kritischer IT- und Energie-Infrastrukturen. In M. Kloepfer (Hrsg.). *Schutz kritischer Infrastrukturen* (67-83). Baden-baden: Nomos.

Schneier, B. (2001). *Managed Security Monitoring: Network Security.* Santa Clara: Counterpane Internet Security, Inc.

Schossing, W. (2007). *Blackouts in der Stromversorgung. 10. Arbeitskreis-Symposium Netzleittechnik "Netzleittechnik im Spiegel sich verändernder wirtschaftlicher Rahmenbedingungen".* Dresden: Verband der Elektrotechnik Elektronik Informationstechnik.

Schubert, S., Vennegeerts, H. & Quadflieg, D. (2008). *Erkenntnisse aus der FNN-Störungsstatistik.* Verfügbar unter http://www.vde.de/de/fnn/arbeitsgebiete/versorgungsqualitaet/documents/vde-kongress_fnn-stoerungsstatistik2008-11-04.pdf [13. September 2010].

Schulze, T. (2006). *Bedingt abwehrbereit - Schutz kritischer Informations-Infrastrukturen in Deutschland und den USA.* Wiesbaden: Verlag für Sozialwissenschaften.

Schwarz, H., Bitsch, R., Fichtner, W., Pforte, R. & Pfeiffer, K. (2008). *Netzintegration Erneuerbarer Energien in Brandenburg. Kurzfassung einer Studie im Auftrag des Ministeriums für Wirtschaft des Landes Brandenburg.* Leibniz Institut.

Shull, A. R. (2006). *Critical Energy Infrastructure Protection Policy Research Series. Assessment of Terrorist Threats to the Canadian Energy Sector.* Ottawa: Canadian Centre of Intelligence and Security Studies.



Statistisches Bundesamt Deutschland (Destatis) (2009). *DE STATIS wissen.nutzen*. Verfügbar unter https://www-genesis.destatis.de/genesis/online;jsessionid=96F8463BB343C19406D02EE7CA6B5418.tomcat_GO_2_2?operation=abruftabelleBearbeiten&levelindex=2&levelid=1283436655194&auswahloperation=abruftabelleAuspraegungAuswaehlen&auswahlverzeichnis=ordnungsstru [02. September 2010].

Stober, R. (2010). Der Beitrag der Sicherheitswirtschaft und der Unternehmen zum Schutz kritischer Infrastrukturen. In M. Kloepfer (Hrsg.). *Schutz kritischer infrastrukturen* (121-132). Baden-Baden: Nomos.

sueddeutsche.de (2010). *Zwei Tote bei Anschlag auf Pipeline in der Türkei.* Verfügbar unter http://www.sueddeutsche.de/politik/politik-kompakt-obama-kandidat-siegt-in-colorado-1.986762-4 [22. September 2010].

Tagwerker, G. (2004). *Chronologie und Ursachen der großen Stromausfälle in Europa 2003.* Wien: Österreichische Gesellschaft für Europapolitik.

Thierauf, G. (2006). *Gutachten zur Ermittlung der Schadensursache der am 25./26.11.2005 im westlichen Münsterland geschädigten Stahlgittermaste des Hoch- und Mittelspannungsnetzes.* Essen.

Thywissen, K. (2006). *Components of Risk. A Comparative Gossary.* United Nations University Institute for Environment and Human Security. Bonn: United Nations University Press.

Turner, B.L., Kasperson, R.E., Matson, P.A., McCarthy, J.J., Corell, R.W., Christensen, L., Eckley, N., Kasperson, J.X., Luers, A., Martello, M. L., Polsky, C., Pulsipher, A. & Schiller, A. (2003). A framework for vulnerability analysis in sustainability science. *Proceedings of the National Academy of Science of the United States of America, 100* (14), 8074-8079.

Union for the Co-ordination of Transmission of Electricity (UCTE) (2007). *Final Report - System Disturbance on 4 November 2006.* Brussel: Union for the Co-ordination of Transmission of Electricity.

Union for the Co-ordination of Transmission of Electricity (UCTE) (2008). *UCTE Transmission Development Plan.* Brussel: Union for the Co-ordination of Transmission of Electricity.

United Nations International Strategy for Disaster Reduction (UN/ISDR) (2004). *Living with Risk: A global review of disaster reduction initiatives.* United Nations International Strategy for Disaster Reduction. Geneva: United Nations publications.



United Nations International Strategy for Disaster Reduction (UN/ISDR) (2009). *UNISDR Terminology on Disaster Risk Reduction.* Verfügbar unter von http://www.unisdr.org/eng/library/lib-terminology-eng.htm [23. September 2010].

United Nations Development Programme (UNDP) (2004). *Reducing Disaster Risk: A Challenge for Development. A Global Report.* United Nations Development Programme. New York: John S. Swift Co.

van der Vleuten, E. & Lagendijk, V. (2010). Transnational infrastructure vulnerabilty: The historical shaping of the 2006 European "Blackout". *Energy Policy, 38 (4),* 2040-2052.

Verband der Elekrotechnik Elektronik Informationstechnik (VDE) (2008). *Smart Distribution 2020: Virtuelle Kraftwerke in Verteilungsnetzen*. Verfügbar unter http://www.e-energy.de/documents/VDE_Studie_Smart_Distribution.pdf [21. September 2010].

Verband der Elektrotechnik Elektroknik Informationstechnik (VDE) (2010). *Nichtverfügbarkeit 2008*. Verfügbar unter http://www.vde.de/de/fnn/arbeitsgebiete/versorgungsqualitaet/Documents/Uebersicht_Nichtverfuegbarkeit_2007_2008.pdf [17.08.2010].

Verband der Netzbetreiber (VDN) (2006). *VDN-Verfügbarkeitsstatistik - Berichtsjahr 2006.* Berlin: Verband der Netzbetreiber.

Verband der Netzbetreiber (VDN) (2007). *VDN-Störungs- und Verfügbarkeitsstatistik.* Berlin: Verband der Netzbetreiber.

Villagrán de León, J. C. (2006). *Vulnerability. A Conceptual and Methodological Review.* Bonn: United Nations University - Institute for Environment and Human Security.

Watts, D. (2003). *Security & Vulnerabilty in Electric Power Systems.* Rolla: NAPS 2003, 35th North American Power Symposium.

Weichselgartner, J. (2000). Hochwasser als soziales Ereignis. Gesellschaftliche Faktoren einer Naturgefahr. *Hydrologie und Wasserbewirtschaftung, 44* (3), S. 122-131.

Wilson, C. (2005). *Defense Program Issue: Global Information Grid, Bandwidth Expansion (GIG-BE).* Washington: CRS Report for Congress.

Wisner, B., Blaikie, P., Cannon, T. & I. Davis (2004). *At Risk: Natural Hazards, People's Vulnerability and Disasters*. (2. Auflage). London: Routledge.

Wissner, M. (2010). ICT, growth and productivity in the German energy sector - On the way to a smart grid? *Utilities Policy,* 1-6.



Zebisch, M., Grothmann, T., Schröter, D., Hasse, C., Fritsch, U. & Wolfgang, C. (2005). *Klimawandel in Deutschland. Vulnerabilität und Anpassungsstrategien klimasensitiver Systeme*. Dessau: Umweltbundesamt.

Zimmermann, R. (2004). *Decision-Making and the Vulnerability of Interdependent Critical Infrastructure*. Los Angeles: Center for Risk and Economic Analysis of Terrorism Events.



www.schriftenreihe-sicherheit.de